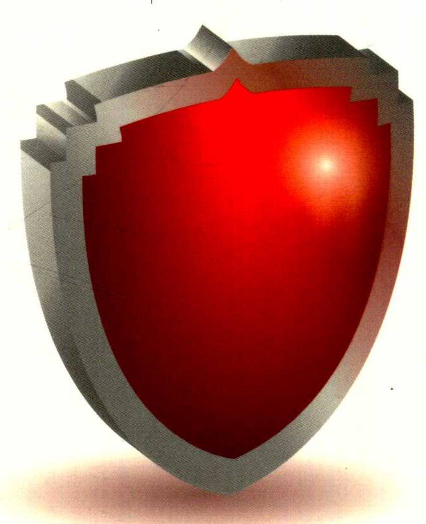


"十三五"
国家重点图书出版规划项目
ICT认证系列丛书

华为技术认证

华为Anti-DDoS技术漫谈

韩 姣 主编







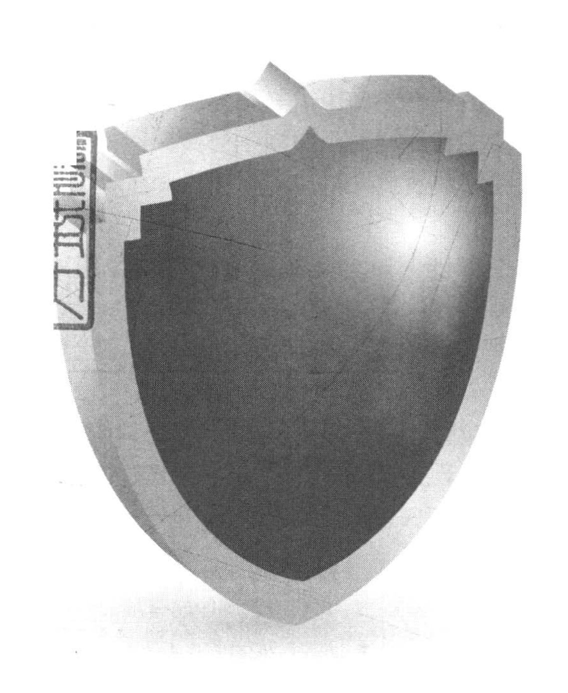




华为技术认证

华为Anti-DDoS技术漫谈

韩 姣 主编



人民邮电出版社
北 京

图书在版编目（CIP）数据

华为Anti-DDoS技术漫谈 / 韩姣主编. -- 北京 : 人民邮电出版社, 2018.8
（ICT认证系列丛书）
ISBN 978-7-115-48754-4

Ⅰ. ①华… Ⅱ. ①韩… Ⅲ. ①计算机网络－计算机安全 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第132783号

内容提要

本书以现实网络中的热点攻击事件为入口，深入分析了各种 DDoS 攻防原理，并结合华为 Anti-DDoS 技术给出了详细解决方案。同时，作者总结多年维护和服务经验，将其作为配置要点呈献给读者，内容涵盖华为 Anti-DDoS 解决方案的组成、产品介绍、要点配置和实战案例等。

本书适合于服务或者渠道工程师，以及想学习或对 DDoS 攻防技术感兴趣的读者；同时，本书也可作为理论学习用书，帮助企业员工学习 Anti-DDoS 技术，帮助他们熟悉和理解华为 Anti-DDoS 的相关技术应用，提升工作效率。

◆ 主　　编　韩　姣
责任编辑　李　静
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：16　　　　2018 年 8 月第 1 版
字数：230 千字　　　　2018 年 8 月北京第 1 次印刷

定价：59.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

随着云计算的快速发展，各行各业的业务越来越多地向云化转变，DDoS 攻击已经成为互联网的首要威胁。越是竞争激烈的在线业务，被攻击的频度越高，攻击越复杂。随着 IoT 的快速发展，越来越多的 IoT 终端成为攻击端，由于各类开放服务器放大了攻击，攻击流量峰值也越来越高。目前，多矢量混合攻击更成为常态，在这种形势下，DDoS 攻防对抗技术难度一再被提升。另一方面，易遭受攻击的游戏、视频聊天等应用，大多采用私有协议，私有协议的广泛使用也进一步提升了防御技术的难度。

当 DDoS 防御作为一种 SaaS 服务企业客户时，防御系统不仅要求它能快速响应攻击，还要求它在过滤攻击时尽可能降低客户对访问体验的影响。因此，当前的 DDoS 防御技术远不是限速和 SYN Cookie 那么简单。一个好的防御系统应当有丰富多样的防御策略，即使对于同一类攻击，针对不同的业务系统也可提供不同的防御策略。但丰富灵活的防御策略也是把双刃剑，对懂这些技术的人而言，丰富灵活的防御策略提供了更多的运维手段；而对不懂这些技术的人来说，防御策略的配置太复杂，配置不当往往容易引起防御误判。配置复杂和运维成本高，已成为 DDoS 防御系统的代名词。因此，运维人员对攻防技术原理理解的深入程度直接决定了防御系统发挥作用的大小。而且 DDoS 防御方案的部署对网络有很强的依赖性，不同的网络需要不同的引流回注方案，如何实现 Anti-DDoS 方案在典型场景的快速部署，同样是安全运维或交付人员需要掌握的基础知识。

华为 16 年安全产品的成功经验，不仅奠定了华为在信息安全领域的地位，同样造就了一支精锐的安全产品研发团队。华为一贯重视产品资料，要求服务团队、客户甚至资料团队能按照资料说明，完成设备上线，这一近乎无情的苛刻要求无形中造就了华为安全产品资料团队人人都是安全专家。《华为 Anti-DDoS 技术漫谈》是继《华为防火墙技术漫谈》之后的华为安全产品资料团队推出的又一精品力作，是华为 Anti-DDoS 产品资料专家团队在华为 10 多年的 DDoS 攻防技术持续研究及 Anti-DDoS 产品研发经验的基础上，推出的一本难得的针对企业安全运维人员的 DDoS 攻防技术教科书。本书用幽默、形象的语言，结合现网几次著名攻击事件，深入浅出地揭开每一种攻击防御技术神秘的面纱，让安全运维人员理解攻击本质，掌握防御技术要点，同时结合典型防御场景，总结 Anti-DDoS 方案部署的要点，为从前期网络规划到后期部署、策略配置，提供了详细的配置举例说明。

最初，华为 Anti-DDoS 产品资料专家团队只是将每一种攻防技术内容在华为企业论坛上分期发表，没想到此项举措引起业内外人士广泛关注，好评如潮。因而团队萌发了将其装订成册的想法，让它以 DDoS 攻防专业技术书籍的形式呈现给华为的客户，期望华为 10 多年的 DDoS 攻防技术积累能直接使客户的网络更加安全。

华为 Anti-DDoS 产品经理　杨莉

前　言

适用读者对象

- 华为 Anti-DDoS 方案的用户

本书可作为华为 Anti-DDoS 用户的自学用书，帮助他们更快地熟悉 Anti-DDoS 方案，了解 Anti-DDoS 方案的关键防御原理，掌握 Anti-DDoS 方案部署技巧，找到解决问题的思路。

- ICT 从业人员

本书可作为工具用书，帮助 ICT 从业人员更快地熟悉 Anti-DDoS 方案，了解 Anti-DDoS 方案关键防御原理，掌握 Anti-DDoS 方案部署技巧，找到解决问题的思路。

本书可作为 HCIE 安全培训认证参考书，帮助 ICT 从业人员尽快通过华为认证，提升个人价值。

- 高校学生

本书可作为计算机通信等相关专业学生的自学参考书，帮助学生快速地熟悉 Anti-DDoS 防御技术，使他们在今后的职业生涯中有一个更好的起步。

- 对信息和网络技术感兴趣的爱好者

本书可作为学习信息和网络技术的参考书籍，使爱好者了解华为产品和技术的特点，掌握华为产品和技术的应用，并为其进一步的技术研究提供指导。

本书主要内容

全书共分为 7 篇，包括方案篇、DNS 篇、HTTP 篇、TCP 篇、UDP 篇、配置篇和实战篇。方案篇介绍了华为 Anti-DDoS 方案的组成、关键技术及应用场景；DNS 篇、HTTP 篇、TCP 篇、UDP 篇主要通过近几年的几次热点 DDoS 攻击案例，介绍不同协议类型的攻击防御原理；配置篇主要介绍引流和回注的配置要点，以及防御策略的关键配置；实战篇共包含 4 个实际案例，采用了先介绍场景，再介绍配置，一边介绍配置一边点评的写作方式，向读者传授理论应用于实践时的技巧。

第 1 篇　方案

本篇首先介绍了 DDoS 攻击的定义、特点和分类，然后介绍了华为 Anti-DDoS 方案关键技术以及华为云清系统；另外，还介绍了华为 Anti-DDoS 的硬件产品型号、部署方式和部署模式，这些是读者了解华为 Anti-DDoS 方案必须掌握的入门级概念。

第 2 篇　DNS

本篇首先以近几年轰动全国的视频软件断网事件为背景，介绍 DNS 攻击过程以及关键防御思路；然后系统解析 DNS 协议报文的格式和交互过程，并分别介绍华为 Anti-DDoS 方案如何防御 DNS Request Flood 攻击、DNS Reply Flood 攻击以及 DNS 缓存

投毒攻击的原理。

第 3 篇 HTTP

本篇首先通过跨站脚本攻击事件，介绍 HTTP 攻击过程及关键防御思路；然后系统解析 HTTP 请求报文和响应报文的格式和交互方式，并分别介绍华为 Anti-DDoS 方案如何防御 HTTP GET Flood、HTTP POST Flood 以及 HTTP 慢速攻击的原理。

第 4 篇 TCP

本篇首先分析近几年一次较大的 SYN Flood 攻击事件，并引出 SYN Flood 攻击的关键防御思路；然后详细分析 TCP 的报文格式及三次握手和四次握手交互过程，并分别介绍针对 SYN Flood、SYN-ACK Flood、ACK Flood、FIN/RST Flood 攻击的防御原理，以及防御 TCP 连接耗尽攻击和 TCP 异常报文攻击等常见的 TCP 类攻击的原理。

第 5 篇 UDP

本篇首先以近几年越来越猖獗的 NTP 反射放大攻击为背景，介绍反射放大攻击的攻击原理和防御思路；然后在深入分析 UDP 报文格式和报文特点的基础上，介绍华为 Anti-DDoS 方案针对 UDP Flood 攻击的防御关键技术及原理。

第 6 篇 配置

本篇介绍了华为 Anti-DDoS 方案在部署过程中常用的关键配置，包含引流和回注配置、引流回注配置结果验证，以及防御策略和阈值的配置要点等。

第 7 篇 实战

1. 城域网防护

本章介绍了华为 Anti-DDoS 方案部署在城域网出口，如何为城域网提供 DDoS 防护的规划和配置思路，以及结合城域网特点给出配置建议。

2. 小型数据中心防护

本章介绍了华为 Anti-DDoS 方案部署在小型数据中心出口，如何为单链路的数据中心提供 DDoS 防护的规划和配置思路，以及结合单链路数据中心特点给出配置建议。

3. 大型数据中心防护

本章介绍了华为 Anti-DDoS 方案部署在大型数据中心出口，如何为双链路的数据中心提供 DDoS 防护的规划和配置思路，以及结合双链路数据中心特点，从可靠性等多方面考虑给出配置建议。

4. 企业园区防护

本章介绍了华为 Anti-DDoS 方案部署在企业园区出口，如何为企业网提供 DDoS 防护的规划和配置思路，以及结合企业网的特点，从可靠性等多方面考虑给出配置建议。

鸣谢

本书由华为技术有限公司网络资料开发部安全网关资料组编写，经人民邮电出版社出版上市。在此期间，培训认证部的领导、资料部的领导、安全网关产品部的领导给予了很多的指导、支持和鼓励，人民邮电出版社的老师给予了严格、细致的审核。在此，诚挚感谢相关领导的扶持，感谢人民邮电出版社各位编辑老师以及本书各位编委的辛勤工作！

以下是本书主编介绍。

韩姣，具有 10 年华为 Anti-DDoS 产品资料开发经验，负责华为 Anti-DDoS 产品文档的写作。她曾作为《强叔侃强》作者之一，参与《华为防火墙技术漫谈》中攻击防范部分的写作。

以下是参与本书编写和技术审校人员名单。

策　　划：李学昭、金德胜

作　　者：韩姣、白　杰、金德胜、卢宏旺、房雪艳

美术编辑：申洪文

技术评审：杨　莉、吴　波、李　翔、潘永波、胡　伟、黄治登、袁　方、陶倚天、闫广辉、矫翠翠、沈海峰、朱旭德、吴永清、陈　佳、张凯程、邓福祥、姜　昊、付　佳、李　帅

参与本书编写和审稿的老师虽然有多年 ICT 从业经验，但因时间仓促，错漏之处在所难免，望读者不吝赐教，在此表示衷心的感谢。读者对于本书有任何意见和建议可以发送邮件至 hanjiao09@huawei.com，或直接登录华为企业论坛《华安解密》汇总帖反馈。

目　　录

第1篇 方案

1.1 什么是 DDoS 攻击

1.1.1 DDoS 攻击的定义

DDoS 的前身是 DoS（Denial of Service，拒绝服务），最基本的 DoS 攻击是指攻击者利用大量合理的服务请求来占用过多的攻击目标的服务资源，从而使合法用户无法得到服务响应的过程。DoS 攻击一般采用一对一的方式，当攻击目标各项性能指标不高时（例如 CPU 速度低、内存小或者网络带宽小等），它的效果是明显的，如图 1-1 所示。

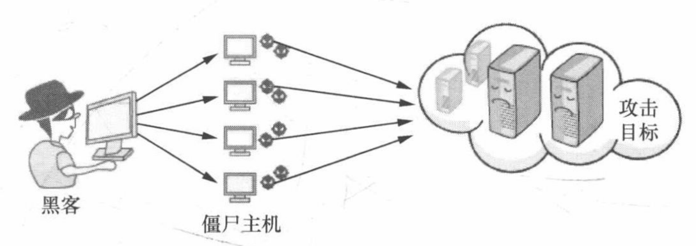


图 1-1 DDoS 攻击过程示意

随着计算机处理能力的不断提高，网络带宽迅速增长，以往的受攻击目标对这些恶意请求的“消化能力”增强了很多，这就使得 Dos 攻击的困难程度大大增加。一个攻击者无法使目标“拒绝服务”，那么攻击者会同时发起多个攻击，这时 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击也就应运而生了。DDoS 攻击是指攻击者控制僵尸网络中的大量僵尸主机向攻击目标发送大流量数据，耗尽攻击目标的系统资源，导致其无法正常地响应服务请求。

1.1.2 DDoS 攻击的特点

1. DDoS 攻击很容易被发起

DDoS 攻击的发起很容易，攻击者可以很方便地从互联网获取各类 DDoS 攻击工具，从而发起攻击。比较出名的发起 DDoS 的免费工具有卢瓦（LOIC）、HOIC（LOIC 升级版）、XOIC、Hulk、DAVOSET、黄金眼等。DDoS 攻击者还可以购买僵尸网络或者 DDoS 攻击服务，有的攻击者甚至可以借助正常的软件或网站发起攻击。

2. DDoS 攻击防御难度大

DDoS 攻击防御难度大，攻击会损害受害者的金钱、服务和信誉。报告显示，65% 以上的 DDoS 攻击每小时给受害企业造成的损失高达一万美元。例如 2016 年 10 月，针对美国 DNS 服务提供商 Dyn 公司的一系列 DDoS 攻击导致 Twitter、GitHub、BBC、华尔街日报、Xbox 官网、CNN、HBO Now、星巴克、纽约时报、The Verge、金融时报等大量站点无法正常访问，造成的损失不可估量。

1.1.3　DDoS 攻击的分类

DDoS 攻击根据攻击方式划分有以下三种类型：泛洪攻击（Flood）、畸形报文攻击（Malformation）和扫描探测类攻击（Scan&Probe）。

1. 泛洪攻击

泛洪攻击是一种攻击者通过僵尸网络、代理或直接向攻击目标发送大量伪装的服务请求报文，最终耗尽攻击目标的资源的攻击方式，如图 1-2 所示。攻击者发送的大量报文可以是 TCP 的 SYN 和 ACK 报文、UDP 报文、ICMP 报文、DNS 报文、HTTP/HTTPS 报文等。

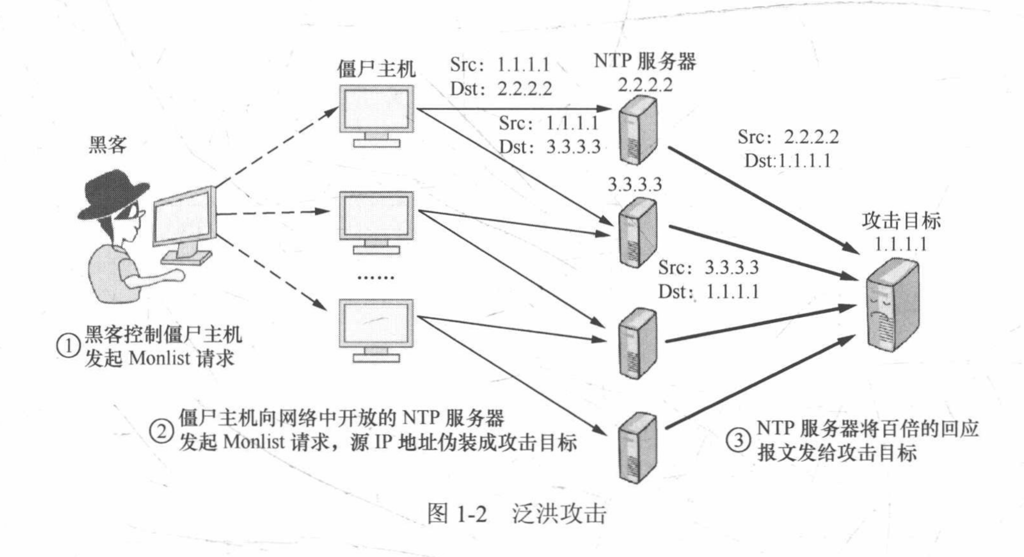


图 1-2　泛洪攻击

近年来，泛洪攻击又发展出了一种高级形式，即反射攻击。反射攻击并不是攻击者直接向攻击目标发起大量的服务请求，而是攻击者控制僵尸网络中的海量僵尸主机，将其伪装成攻击目标，然后这些僵尸主机以攻击目标的身份向网络中的服务器发起大量服务请求。网络中的服务器会响应大量的服务请求，并发送大量的应答报文给真正的攻击目标，从而造成真正的攻击目标性能耗尽。

反射攻击大多是由 UDP flood 变种而来的，它反射的是 UDP 报文，例如 NTP、DNS、SSDP、SMTP、Chargen 等。攻击者为什么会选中 UDP 报文呢？因为 UDP 的响应（Response）报文大小要大于请求（Request）报文，这样攻击者就实现了放大攻击流量的目的。

以 NTP 报文为例，NTP 的 Monlist 命令被用来查询最近所有和服务器通信的记录，服务器会返回最多 600 个通信记录，这样流量就被放大了数百倍。如果攻击者控制成千上万的僵尸主机，并将其伪装成攻击目标，并向 NTP 服务器发送大量此命令，那么反射给攻击目标的流量数量可想而知！

2. 畸形报文攻击

畸形或特殊报文攻击通常是指攻击者发送大量有缺陷或具有特殊控制作用的报文，从而造成主机或服务器在处理这类报文时造成系统崩溃的过程。常见的畸形报文攻击有

Smurf、Land、Fraggle、Teardrop、WinNuke 攻击等。特殊控制报文攻击包括超大 ICMP 报文、ICMP 重定向报文、ICMP 不可达报文和各种带选项的 IP 报文攻击。

3. 扫描探测类攻击

扫描探测类攻击是一种潜在的攻击行为，并不具备直接的破坏行为。它通常是指攻击者发动真正攻击前的网络探测行为，例如 IP 地址扫描和端口扫描等。

DDoS 攻击从网络层次的划分见表 1-1。

表 1-1 攻击分类

网络层次	DDoS 攻击
网络层	IP 地址扫描攻击 大部分特殊控制报文攻击 Teardrop 攻击 Smurf 攻击 IP 分片报文攻击 ICMP flood 攻击
传输层	SYN flood SYN-ACK flood ACK flood FIN/RST flood TCP 连接耗尽攻击 UDP flood（包括各种反射攻击） TCP/UDP 分片报文攻击 DNS flood DNS 缓存投毒 其余各种与 TCP、UDP 报文和端口相关的攻击
应用层	HTTP flood HTTP 慢速攻击 HTTPS flood SSL DDoS 攻击 SIP flood

1.1.4 DDoS 攻击分析

1. DDoS 攻击类型

通过以上描述，大家应该对 DDoS 攻击有了初步的了解。下面我们再为大家分析一下当前 DDoS 攻击的趋势，让大家对我们当今所处的网络环境中的 DDoS 攻击有一个初步的认识。

如图 1-3 所示，华为未然实验室现网络攻击事件统计数据显示，SYN flood、UDP flood（包括 UDP 类反射放大攻击）、HTTP get flood、DNS query flood 等依然是 DDoS 攻击的惯用手段。

（1）SYN flood

SYN flood 攻击是 DDoS 攻击中的经典方式，也是最古老和原始的 DDoS 攻击方式。在网络发展初期，SYN flood 攻击就是 DDoS 攻击的代名词。SYN flood 攻击具有攻击简

单、防御难的特质。SYN flood 攻击使用的是最简单、最常用的、被用于 TCP 三次握手的 SYN 报文，所以其发起攻击十分简单；而且，SYN 报文是 TCP 连接建立的第一个报文。单独来看，每一个 SYN 报文都是正常的，防御设备不会对其采取任何措施。

（2）UDP flood

UDP flood 攻击目前已经取代 SYN flood 攻击，成为 DDoS 攻击中的主要方式。具体原因如下：第一，UDP 都是无连接的协议，不提供可靠性和完整性校验，因此其成为攻击者理想的利用对象；第二，UDP 种类繁多，防御起来难度更大；第三，传统 UDP 攻击是攻防者之间关于带宽的比拼，而反射型的 UDP 攻击让攻防者不再对等，因为反射出来的攻击流量要远远大于攻击者投入的流量。

（3）HTTP flood

HTTP flood 攻击迅速发展的原因如下：第一，HTTP 的应用十分广泛；第二，网页和应用中的漏洞比较容易被攻击者利用构造 HTTP 反射类的攻击。例如，攻击者在海量访问的网页中嵌入指向攻击目标网站的恶意 JavaScript 代码，当互联网用户访问该网页时，流量会被反射到攻击目标网站。

（4）DNS flood

DNS flood 攻击 DNS 服务器的代价小，影响范围广，能够造成恐慌，因此此类攻击仍占有较大比例。

2. DDoS 攻击目标

DDoS 的攻击目标主要为游戏、电子商务、互联网金融等，如图 1-4 所示。这些都是利润较高的行业，且是竞争最激烈的行业。因此恶意竞争是目前 DDoS 攻击的主要动机。利润越高、竞争越激烈的行业，遭受攻击的频率越高。

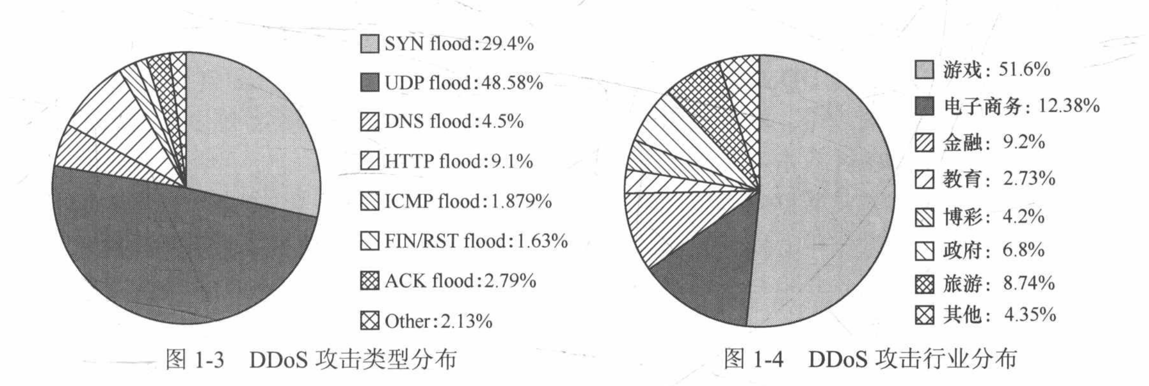


图 1-3　DDoS 攻击类型分布

图 1-4　DDoS 攻击行业分布

游戏行业作为近几年兴起的新兴行业，已经成为 DDoS 攻击的“重灾区”。游戏行业也是竞争最激烈的行业之一，在线游戏和直播网站一旦被攻击，玩家将直接掉线，由此带来的损失非常大。游戏行业用户基数大、用户类型多、在线维护难度大的特点，也使其极易受到 DDoS 攻击。另外，由于很多游戏是基于私有协议开发的，传统的 DDoS 防御手段在没有贴合业务特性的情况下，防御 DDoS 攻击较难。

3. DDoS 攻击的趋势

DDoS 攻击的趋势总结起来主要有 4 点，如图 1-5 所示。





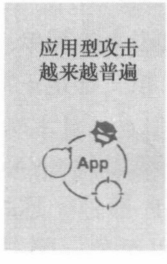




图 1-5 DDoS 攻击趋势

（1）攻击流量越来越大

DDoS 的攻击流量已达 500Gbit/s。2016 年全球有记录的 DDoS 峰值已近 60Gbit/s，而到了 2017 年上半年，规模最大的 DDoS 攻击流量则已达到 650Gbit/s。其中，游戏行业大于 30Gbit/s 以上的攻击就超过了 1800 次。

（2）移动攻击越来越多

随着智能终端和 4G 移动网络的普及，来自移动端的攻击越来越多。移动终端的安全防护能力和用户安全意识较弱，容易成为 DDoS 攻击利用的对象。值得一提的是，随着物联网的兴起，基于物联网协议的 SSDP（Simple Service Discovery Protocol）的反射攻击频率越来越高，明显超越 NTP、DNS 等传统反射攻击。SSDP 被广泛应用于网络摄像头和智能家电，因此 SSDP 反射攻击源数量非常庞大，而且网络资源更加丰富。

（3）应用型攻击越来越普遍

应用层的攻击将会越来越普遍。报告显示，2017 年与 2016 年相比，应用型攻击增长了 42%。其中 HTTP flood 攻击增长高达 26%，混合型攻击增长高达 40%。

混合型攻击是指攻击者同时采取多种类型的攻击报文来进行 DDoS 攻击，例如，传输层与应用层相结合的 DDoS 攻击，应用层的 HTTP flood 大流量攻击与 HTTP 慢速小流量渗透攻击相结合的攻击。混合型 DDoS 攻击让普通的 DDoS 防御设备难以防范，或将成为今后主流的 DDoS 攻击方式。

（4）攻击更多是从数据中心发起的

报告显示，由数据中心向外发起的 DDoS 攻击呈增长趋势；数据中心服务器被黑客控制沦为僵尸网络的趋势也与日剧增；超大流量的 DDoS 攻击多数由被控制的数据中心发起。由此可见，数据中心已经成为 DDoS 攻击的控制目标。

随着云计算的快速发展，互联网业务越来越集中，云数据中心将面临比传统数据中心更加严峻的 DDoS 攻击考验。主要原因在于：云数据中心虚拟机的租户身份难以被有效识别，且其安全意识薄弱；虚拟机数量庞大、业务种类多、流量模型差别大，难以得到完全的、具有针对性的防护。

1.2 华为 Anti-DDoS 方案

前面我们介绍了 DDoS 攻击的基本概念并分析了 DDoS 攻击的发展趋势。可能大家

会考虑，对于 DDoS 攻击，我们难道就没有应对之策了吗？

在这种情况下，华为 Anti-DDoS 方案应运而生，其能够完美地检测和防御 DDoS 攻击，是当今对抗 DDoS 攻击的不二之选。

1.2.1　华为 Anti-DDoS 方案的介绍

华为 Anti-DDoS 方案包括三大组件：检测中心、清洗中心和管理中心（ATIC）。

① 检测中心主要负责检测流量，发现流量异常后上报管理中心，管理中心下发引流策略至清洗中心，指挥清洗中心进行引流清洗。

② 清洗中心主要根据管理中心下发的策略进行引流、并清洗流量（过滤），并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。

③ 管理中心负责检测中心和清洗中心的统一管理和调度，即日志记录和报表呈现，以及 Anti-DDoS 运营方案的提供。

华为 Anti-DDoS 方案的经典部署如图 1-6 所示。

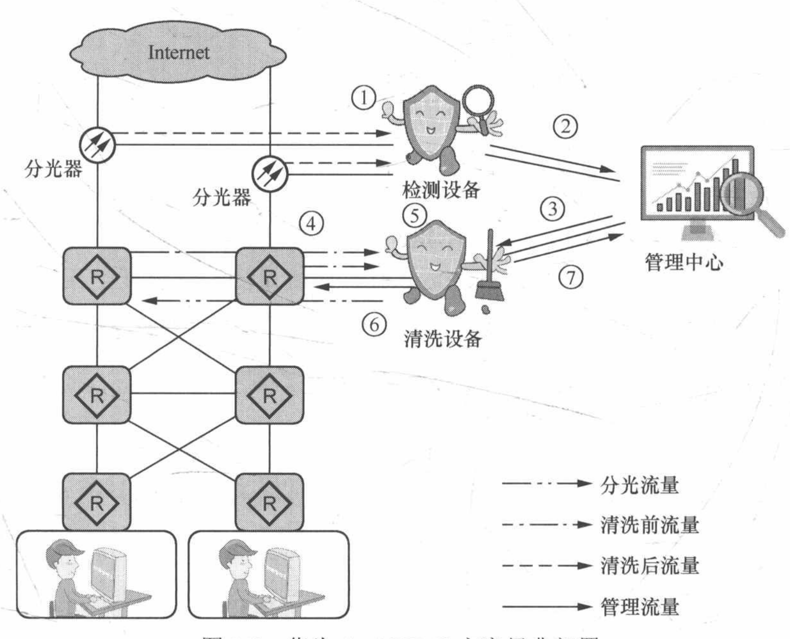


图 1-6　华为 Anti-DDoS 方案经典部署

Anti-DDoS 方案的工作流程说明如下。

① 检测中心检测分光或者镜像流量。

② 检测中心发现流量异常后，上报受攻击的 IP 地址到管理中心。

③ 管理中心自动向清洗中心下发引流策略。

④ 清洗中心根据引流策略将去往被攻击 IP 地址的流量引流到清洗中心中。

⑤ 清洗中心通过先进的多层过滤防御技术清洗流量，丢弃攻击流量。

⑥ 清洗中心将清洗后的正常流量回注到网络中。

⑦ 清洗中心上报攻击日志到管理中心，管理中心负责呈现流量清洗效果。

1.2.2 动态流量基线技术

常见的 DDoS 攻击主要是大流量的攻击，因此检测中心的主要工作是分类统计流量，然后和预先配置的检测阈值进行比较，如果流量超过检测阈值则认为流量发生异常，需要进行清洗。由此可见，检测是否准确主要取决于检测阈值的配置是否合理，而其合理性完全取决于网络安全工程师的经验。不同网络流量的模型不同，因此，检测阈值的配置没有统一的经验值可循。既然检测阈值这么重要，手工配置又这么艰难，而检测设备又永远在线，是否有一种技术可以自动学习网络的各种流量阈值呢？因此，动态流量基线技术应运而生。

华为 Anti-DDoS 系统可周期性地统计学习用户网络流量，其将学习到的周期内每种流量模型的最大值作为基本值，然后再结合容忍度（以防止流量瞬时的抖动引起的误判）计算出最终的攻击检测阈值。当用户网络流量模型发生变化时，流量模型学习结果会自动被调整，相应的检测阈值也会自动被调整。

1.2.3 逐流与逐包检测技术

华为 Anti-DDoS 方案的检测中心有逐流检测和逐包检测两种检测方式。简单来说，逐流检测是抽样检测，而逐包检测是全流量的检测，不同的检测形态可以对应不同的场景。

1. 逐流检测

逐流检测是指检测中心收集、分析网络中路由交换设备发出的 Netflow 日志，并根据 Netflow 日志来检测 DDoS 攻击。Netflow 日志是流量的抽样统计结果，它主要包含报文五元组、长度、TCP Flag、流量统计信息（包速率、带宽）等。由于 Netflow 日志不包含应用层信息，因此它无法检测应用层攻击。逐流检测适合超大流量攻击检测的场景，例如，城域网或运营商网络。

2. 逐包检测

逐包检测是指检测中心会逐一地统计和分析所有报文，实现 100%全流量检测。因此逐包检测除了能分析报文的五元组、长度、TCP Flag，流量统计信息外，还能分析报文 3～7 层的信息，包括 TCP 会话行为、应用层协议信息（HTTP、HTTPS、DNS、SIP）和访问行为等。逐包检测适合更精细化的检测与防护场景，例如，数据中心边界或 Anti-DDoS 运营场景。

华为 Anti-DDoS 方案支持丰富的逐包检测功能，可以很好地应对来自应用层的攻击。其具有 5 种统计维度：qps、pps、bit/s、cps、TCP-Ratio。

① qps：qps（Queries Per Second）指定触发攻击防范的 HTTP 报文速率的阈值，统计除 SYN、SYN-ACK、ACK 以外的其他 HTTP 报文。

② pps：pps（Packets Per Second）是指每秒发送的报文数。

③ bit/s：bit/s（Byte Per Second）是指每秒发送的字节数。

④ cps：cps（Connections Per Second，每秒连接数）即新建速率。

⑤ TCP-Ratio：SYN 报文与（SYN+ACK）报文的比例。

同时，华为 Anti-DDoS 还有 8 种协议族：IP、TCP、UDP、ICMP、HTTP、HTTPS、

DNS 和 SIP。38 种协议状态：TCP Flags、TCP connections、TCP window size、HTTP connections、HTTP URI、HTTP Host、SSL Renegotiating、DNS query、DNS domain 等。62 种流量模型：TCP SYN pps、UDP packet bit/s、DNS pps、SIP pps、ICMP pps、TCP FIN pps、TCP ACK pps 等。

1.2.4　多层过滤防御技术

华为 Anti-DDoS 方案采用精细化多层过滤防御技术，不仅能够有效检测和过滤超出阈值的流量，还能够检测并过滤精巧的小流量攻击（例如，慢速攻击、DNS 缓存投毒攻击等）和单包攻击（主要是畸形和控制报文攻击），如图 1-7 所示。

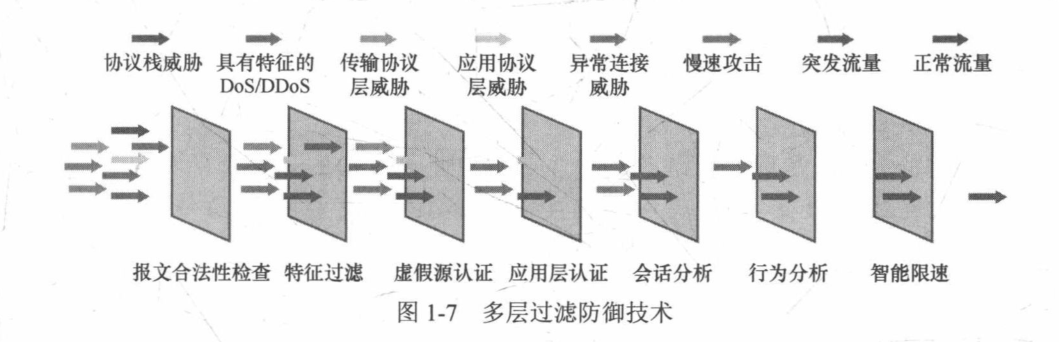


图 1-7　多层过滤防御技术

多层过滤防御技术是华为 Anti-DDoS 方案的核心技术，下面我们一起来学习每层能够过滤的攻击以及基本实现原理。

1. 报文合法性检查

报文合法性检查是基于 RFC 检查报文合法性的，主要检测或过滤利用协议栈漏洞的畸形报文攻击。这一层类似于空气净化器中的初滤网，主要检测和过滤大部分畸形报文攻击和特殊控制报文攻击。

2. 特征过滤

特征过滤是基于报文特征来检测和过滤攻击的，它被用于防御有特征的攻击，包括 UDP flood、UDP 类反射放大攻击（包括 DNS 反射放大、NTP 反射放大等）。特征也被称作指纹，UDP 类攻击流量通常都具有一定的特征。UDP 报文的数据段、源 IP 地址、源端口、目的 IP 地址、目的端口都可能隐藏着攻击报文的特征。例如，UDP 反射放大攻击一般都是基于特定的 UDP 端口，比如现在比较常见的 NTP、DNS、SSDP 反射放大攻击，分别对应 UDP 的 123、53、1900 端口。

华为 Anti-DDoS 方案支持静态指纹和动态指纹。

（1）静态指纹

静态指纹是已知的攻击特征，系统已经预先定义好了攻击特征的参数，并将其保存在过滤器模板中。例如，Anti-DDoS 系统提供了 14 种常见的 UDP 反射放大攻击的过滤器模板。Anti-DDoS 系统会检测 UDP 报文的特征，如果 UDP 报文的特征与过滤器模板中的攻击特征匹配，系统会丢弃此 UDP 报文，并将攻击源加入黑名单。

华为安全智能云中心负责 Anti-DDoS 设备的静态指纹的维护和升级，保证设备能够

快速应对各类新型的 DDoS 攻击威胁。

（2）动态指纹

动态指纹是 Anti-DDoS 系统自动学习获得的特征。动态指纹学习就是系统对一些有规律的 UDP 攻击报文负载进行识别的过程，系统自动提取出相同的内容作为指纹特征，然后把这个提取的特征作为过滤条件，自动应用并进行过滤。例如，一些攻击工具发起的 UDP 攻击，攻击报文通常都拥有相同的字段，比如都包含某一个字符串，或整个报文内容一致，这些相同的字段会被系统提取出来作为指纹特征。

华为 Anti-DDoS 方案的动态指纹学习过程可以有效地学习到新型 DDoS 攻击的指纹特征，而静态指纹又被预置了流行的僵尸工具的攻击特征，因此华为 Anti-DDoS 方案可以有效地防护各种新型 DDoS 攻击，保护业务的可用性。

3. 虚假源认证

虚假源认证用于防范虚假源发起的传输层攻击，包括 SYN flood、SYN-ACK flood、DNS request/reply flood 攻击等。

SYN flood 攻击是虚假源攻击的典型代表，此类攻击的最显著的特点是海量变源或变源端口的报文被发送到受害主机，耗尽受害主机资源或网络资源。Anti-DDoS 方案对此的应对方法简单而言就是：Anti-DDoS 设备会作为“中介”回应源发出的 SYN 报文，如果源是真实的主机，Anti-DDoS 设备则会继续回应 RST 报文，如果源是攻击者构造的虚假源，Anti-DDoS 设备则无法对其响应，如图 1-8 所示。

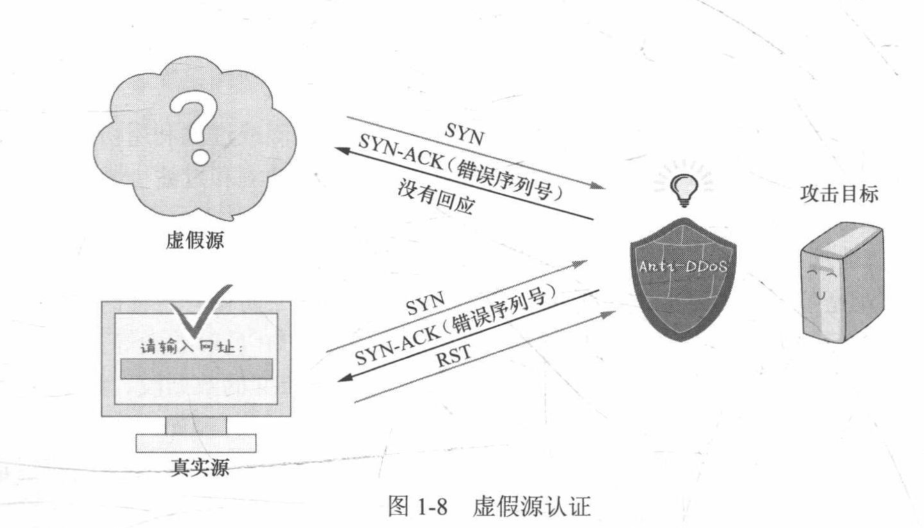


图 1-8 虚假源认证

DNS request flood 和 DNS reply flood 的防御原理也是类似的，Anti-DDoS 系统会向源客户端回应 DNS Reply（Request）报文，然后看客户端是否能正常回应。

4. 应用层认证

应用层认证用于防范虚假源发起的应用层攻击，包括 HTTP get/post flood、HTTPS flood、SIP flood 攻击等。

应用层源认证的防御原理与传输层的防御原理有相似之处。应用层源认证也是

Anti-DDoS 系统作为“中介”回应源客户端的请求，并要求源客户端重定向到新的URL（例如子域名）或者输入验证码，以此来验证客户端的真实性。真实客户端的浏览器可以自动完成重定向过程或由用户输入验证码，通过认证；而虚假源或者一般的攻击工具没有完整的HTTP协议栈，不支持自动重定向功能，更无法输入随机的验证码，因此无法通过认证，如图1-9所示。

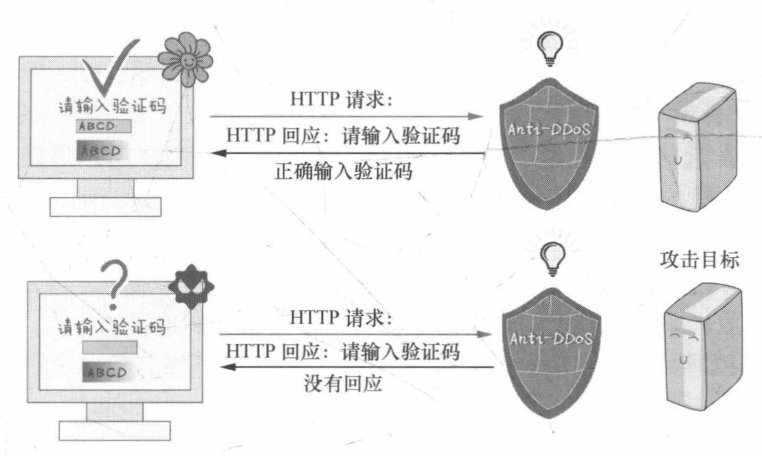


图1-9　验证码认证

5. 会话分析

会话分析基于会话检查并防范会话类攻击，如ACK flood、FIN/RST flood、DNS缓存投毒攻击等。

ACK、FIN、RST等报文都是TCP交互过程中的后续报文，因此Anti-DDoS系统在防御这类报文的泛洪攻击时，可以效仿防火墙对这些报文进行会话匹配检查。真实客户端发出的正常ACK、FIN、RST报文一定能够匹配Anti-DDoS系统上的会话，因为之前Anti-DDoS系统已经为他们的首包SYN报文建立了会话，如图1-10所示。

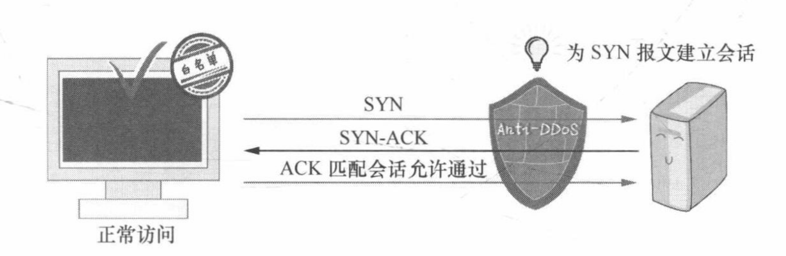


图1-10　真实客户端会话分析结果

如果是攻击者发起的ACK、FIN、RST flood攻击，这些报文将因无法匹配Anti-DDoS系统上的会话而被丢弃，如图1-11所示。

DNS缓存投毒攻击会篡改DNS缓存服务器中的域名与IP地址的对应关系，导致用户访问钓鱼或恶意网站。Anti-DDoS系统的防御原理是为最初的DNS请求报文建立会话，然后检查后续的回应报文是否能够匹配会话。

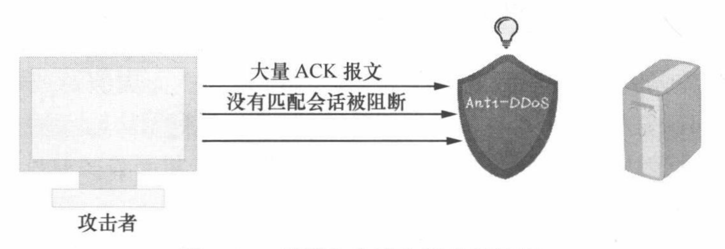


图 1-11　虚假客户端会话分析结果

6. 行为分析

僵尸网络发起的攻击流量和用户访问业务流量行为不同，用户访问流量具有突发性、访问资源分散的特点；而僵尸网络攻击流量的最大特征是访问频率恒定、访问资源固定、访问行为模式固定。因此，我们可以基于行为分析来防御各种慢速攻击。

例如，HTTP 慢速攻击的行为是攻击者在建立了与 HTTP 服务器的连接后，长时间保持连接不释放。系统可以识别分析出这种长期占用 HTTP 连接的行为，从而对其进行阻断，如图 1-12 所示。

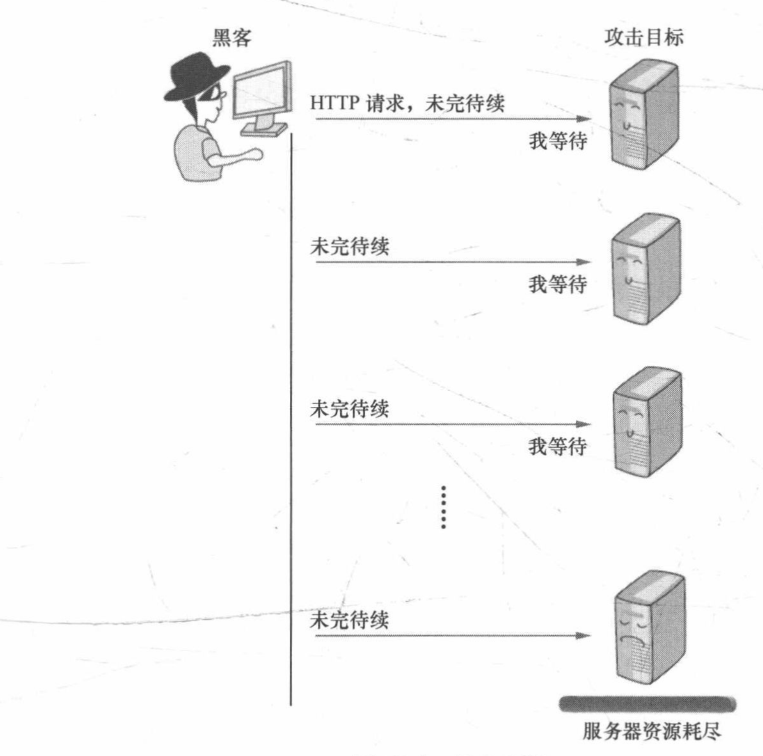


图 1-12　行为分析

7. 智能限速

智能限速采用各类协议精细化限速使得流量都处于安全的带宽范围。流量整形的目的是保证大于阈值的流量都会被检测出来且被调整到合理的数值，即使这些流量在前面的检测中没有出现任何问题。

1.2.5　大数据信誉体系

华为 Anti-DDoS 方案还支持大数据信誉体系，可以使得系统的检测和处理更高效。信誉体系包括全球僵尸网络 IP 信誉库和本地业务访问 IP 信誉库。例如，检测中心发现流量来自僵尸网络的 IP，那么他将直接上报异常给管理中心；而清洗中心在引流后，会快速过滤掉此僵尸 IP 发送的报文，并将其加入黑名单。

① 全球僵尸网络 IP 信誉库是由华为安全智能云中心收集和更新的，目前它已拥有 500 万个僵尸 IP，并且每日动态更新其内容。

② 本地业务访问 IP 信誉库是 Anti-DDoS 系统在防护网络没有遭到攻击时，记忆并学习到的合法流量源的 IP 地址。检测中心将不会检测本地业务访问 IP 信誉库中的地址发出的流量，这充分保证了 Anti-DDoS 系统不会影响网络中常用的正常业务访问，提升了用户体验。

1.2.6　Anti-DDoS 方案运营

随着云数据中心的发展，针对云数据中心和来自云数据中心内部的 DDoS 攻击越来越多。因此 Anti-DDoS 方案必须具备一定的运营能力，它能够提供精细化的防护并提供 DDoS 防护的出租能力。

华为 Anti-DDoS 方案支持多种精细化的防护策略，客户可以为不同的防护对象设置不同的防护策略，从而实现对防护对象的精细化防护。例如，客户可以为 DNS 服务器配置针对 DNS 业务的防护策略，为 HTTP 服务器配置针对 HTTP 业务的防护策略。防护对象是一组被防护的目标 IP 地址，可以是多个 IP/掩码定义的 IP 地址段。防护策略和防护对象都是在 ATIC 上被配置的。

精细化的防护策略和海量的防护对象为 Anti-DDoS 系统的运营提供了基础。客户进行 Anti-DDoS 运营、将 Anti-DDoS 服务进行出租时，可以为不同的租户设定防护对象和配置防护策略。Anti-DDoS 方案还具有租户自助功能，租户可以通过 Portal 服务器自己完成防护对象和防护策略的配置。

Anti-DDoS 系统还提供了丰富的报表功能，既方便管理员阅读分析，又适用于方案的运营。

报表功能支持防护对象、系统两级管理概念的业务数据查询和报表呈现；支持报表手工生成，手工生成报表时，可手工指定数据的时间段；支持以 excel、pdf 格式导出报表；报表粒度包括日报、周报、月报、年报。

1.3　华为云清洗方案与云清洗联盟

华为为了适应网络云化的潮流，推出了更加高端的华为云清洗解决方案。同时，为了共同对抗 DDoS 攻击，华为倡导组织了云清洗联盟。

那么华为 Anti-DDoS 方案、云清洗方案和云清洗联盟之间到底有什么关系呢？本节我们就来一探究竟。

1.3.1 Anti-DDoS 遇到的困难

前文我们分析了 DDoS 攻击呈现出攻击流量逐年上升的趋势，随之而来的是企业防御越来越困难，对抗一次攻击可能需要几个小时甚至几天的时间。同时，为了应对大流量攻击，企业每年需要购置更高性能的硬件设备并扩充运维人员。与此同时，由于攻击的偶然性和不确定性，企业往往需要投入高昂的硬件资源，这样是不具有经济适用性的。

因此，越来越多的企业选择了将对抗 DDoS 攻击的任务托管或部分托管给 MSSP（安全托管服务提供商）来处理，也就是说由云端来处理 DDoS 攻击。MSSP 通常拥有更强大的 DDoS 攻击处理能力，包括更强大的 Anti-DDoS 系统，更专业的安全运维团队等。

MSSP 处理客户 DDoS 攻击的流程如图 1-13 所示。

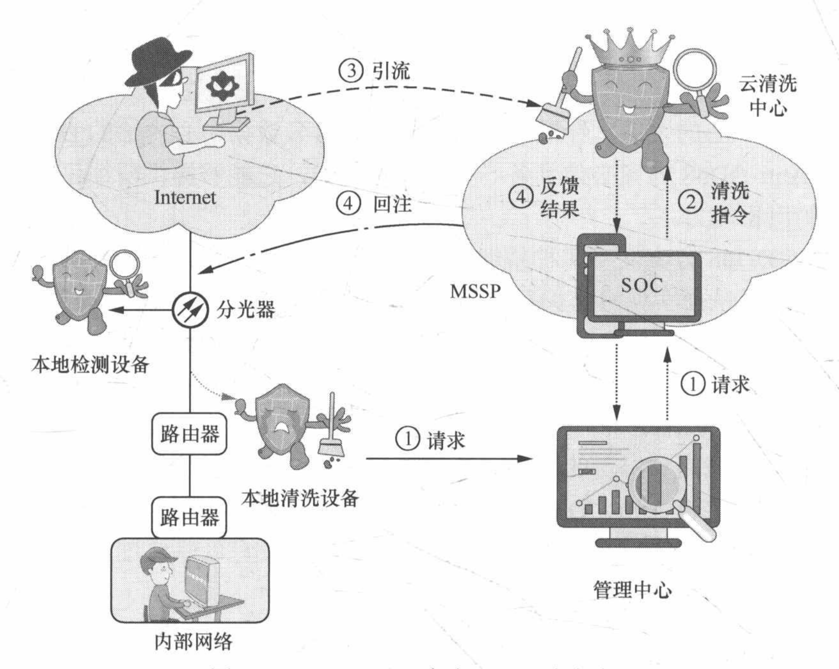


图 1-13 MSSP 处理客户 DDoS 攻击流程

① 客户本地的 Anti-DDoS 系统发现攻击流量达到本地处理能力上限时，会给 MSSP 的 SOC（安全运维中心）系统发送信令，向 MSSP 申请处理 DDoS 攻击。MSSP 的 SOC 收到消息后，会下发清洗指令给清洗中心。

② 清洗中心会将客户的攻击流量引导到自身并进行清洗。

③ 清洗中心清洗完成后，会将清洗后的流量回注给客户，并将清洗结果反馈给 SOC。

④ SOC 收到反馈结果后，会判断攻击是否结束。如果其认为攻击结束，则会通知清洗中心结束本次清洗，并反馈清洗结果和清洗报告给客户。

1.3.2 传统 MSSP 面临的问题

MSSP 解决 DDoS 攻击的问题看似很方便，但也存在问题。

当今僵尸网络具有全球分布的特点，跨越大洲的僵尸网络大量存在。这就导致在同一次 DDoS 攻击事件中，攻击流量来源呈现全球分布性的特点。

例如，客户的 MSSP 只在亚洲部署了清洗中心，而黑客的攻击可能来自于较远的其他大洲。这样亚洲的清洗中心在引流时，会长距离迁移攻击流量，期间可能会造成沿途网络管道拥塞的问题。

由于大量传统的 MSSP 一般只部署一两个清洗中心，因此，大量的攻击流量会在洲际网络间迁移，这就在一定程度上造成了全球一级网络的拥塞，使一级网络充斥着 DDoS 攻击流量。

1.3.3 华为云清洗方案

为了解决传统 MSSP 面临的问题，使 MSSP 能够更好地为客户提供 DDoS 云清洗服务，华为推出了云清洗解决方案。

华为云清洗解决方案主要由本地清洗中心、SOC（Security Operation Center，安全运维中心）和全球的清洗中心组成。本地清洗中心主要处理企业本地普通级别的 DDoS 流量攻击。当企业遭遇大流量 DDoS 攻击时，本地清洗中心会自动识别并触发云信令，请求华为 SOC 调度各地的云清洗中心近源清洗 DDoS 攻击。

华为云清洗解决方案中的本地清洗中心和全球清洗中心其实都可以使用华为 Anti-DDoS 方案。本地清洗中心可以选择 AntiDDoS1600 系列产品，全球清洗中心可以选择 AntiDDoS8000 系列产品。

华为云清洗解决方案的云清洗过程如下。

① 客户本地的清洗中心发现攻击流量达到本地处理能力上限时，会通过 ATIC 发送信令给华为 SOC，向华为 SOC 求助。

② 华为 SOC 收到求助后，会向距离攻击源最近的空闲全球清洗中心下发清洗指令，要求全球清洗中心就近清洗攻击源的攻击流量。

③ 全球清洗中心收到华为 SOC 的清洗指令后，会将就近攻击源的流量引导到自身的清洗中心进行清洗。清洗中心会将清洗后的流量回注给客户，并将清洗结果反馈给华为 SOC。由于实现了攻击流量的就近清洗，攻击流量的迁移距离很近，而且不会跨越洲际网络，因此基本不会造成沿途网络拥塞和一级网络拥塞。

④ 华为 SOC 收到各清洗中心发出的结果后，会判断攻击是否结束。如果它认为攻击结束，则会通知各清洗中心停止本次清洗，并将清洗结果和清洗报告反馈给客户。

通过上述过程我们发现华为云清洗方案的最大特点在于清洗中心遍布全球。确实，目前华为已在全球部署了 10 多家清洗中心。全球部署的清洗中心不仅保证了方案能够实现对全球攻击流量的近源清洗，而且全球清洗中心的联合作业能提供超过 2TB 的强大清洗能力。

除了清洗中心遍布全球外，华为云清洗方案还有两大特点。

（1）能够实现分钟级响应，减小攻击损失

在传统 MSSP 运营模式下，客户需要通过抓包等方法识别出大流量攻击，然后通过电话、邮件等方式通知 SOC 调度清洗资源。整个过程大约需要 2 个小时，效率低下。在

华为云清洗方案中，本地清洗中心可以实时识别大流量 DDoS 攻击，自动触发云信令通知 SOC 执行云清洗操作。SOC 会智能调度当前状态空闲的清洗中心，依照近源清洗的原则清洗攻击流量，整个攻击响应过程无需人工干预，不超过 5 分钟即可完成。

（2）安全服务化交付，降低运维成本

客户只需在网上填写自己的需求，之后就可以快速部署攻击流量清洗网络，他们还可以根据自己的流量清洗要求，购买相应的服务包，按月付费，灵活简单。另外，华为的 7×24 小时的专家团队会帮助客户处理各种紧急突发的攻击情况，客户再也不用为逐年增加的硬件成本和人力投入而烦恼。

华为云清洗解决方案的特点完美地弥补了本地 Anti-DDoS 方案和传统 MSSP 的不足。

1.3.4 云清洗联盟

“云清洗联盟”旨在整合全球运营商、MSSP 和 IDC 的资源，构建一个云端的“DDoS 防御生态系统”。

“云清洗联盟”会通过华为云 SOC 统一管理和调度联盟内的 DDoS 清洗资源，为客户提供强大的 DDoS 近源云清洗服务，同时还可为客户解决上游管道的网络拥塞问题，保护上游带宽。

一个云清洗联盟的运作方式过程如下。

① 例如，MSSP1 和 MSSP2 都是云清联盟的成员，当 MSSP1 客户本地的 Anti-DDoS 系统发现攻击流量达到本地处理能力上限时，系统会发送信令给 MSSP1 的 SOC 系统，向 MSSP1 的 SOC 系统申请处理 DDoS 攻击。

② MSSP1 的 SOC 系统收到信令后，分析发现攻击流量来自两个不同大洲的网络。然而，MSSP1 只在其中一个大洲网络部署了清洗中心，因此，对来自未部署清洗中心大洲的攻击流量，MSSP1 的 SOC 系统会上报云信令给华为云 SOC，申请云清联盟中的清洗中心进行近源清洗。与此同时，对来自部署了清洗中心大洲的攻击流量，MSSP1 的 SOC 系统也会调度自己所部署的清洗中心进行引流清洗。

③ 华为云 SOC 收到 MSSP1 的请求信令后，会根据调度算法选择拥有所需清洗中心的 MSSP2 来处理此请求。华为云 SOC 会给 MSSP2 的 SOC 下发清洗指令，要求 MSSP2 的 SOC 调度距离攻击源最近的清洗中心，对来自 MSSP1 未部署清洗中心大洲的攻击流量进行引流和清洗。

④ MSSP2 的 SOC 收到清洗指令后，会调度清洗中心对来自 MSSP1 未部署清洗中心大洲的攻击流量进行引流和清洗。

⑤ MSSP1 和 MSSP2 的清洗中心引流清洗完成后，会将清洗后的流量回注给客户。

在上述过程中，我们发现云清洗联盟成员 MSSP1 借助联盟为他的客户提供了面向全球的 DDoS 云清洗服务，实现了对客户攻击流量高效快捷的近源清洗。而云清洗联盟成员 MSSP2 由于为 MSSP1 贡献了 DDoS 清洗服务，也将获得 MSSP1 的分成收益。MSSP1 和 MSSP2 通过云清洗联盟实现了双赢的结果。

可见，加入云清洗联盟的企业既可以为自己的客户提供面向全球的 DDoS 云清洗服

务，还可以通过为其他成员提供清洗服务而获得收益，同时还能提升自己在全球 DDoS 防护领域的品牌价值和影响力。

另外，从长远来看，MSSP 加入云清联盟可以将自身安全服务能力展现给更多最终客户，获得更多市场机会，还能够及时获得全球 DDoS 攻击态势、网络攻击数据和趋势分析，以实现安全服务能力的持续提升。

1.4 华为 Anti-DDoS 产品集

互联网和物联网的迅猛发展使我们受益颇深。网络资源在一定程度上已成为孕育 DDoS 攻击的温床。

在 10 余年的被攻击中，华为 Anti-DDoS 解决方案已进化为可以精准防御 100 多种应用型攻击的"产品集"。

1.4.1 解决方案组成

华为自主研发的检测中心、清洗中心、ATIC 实现了 Anti-DDoS 解决方案的核心保障能力。其中，Anti-DDoS 解决方案是指检测中心和清洗中心两部分，如图 1-14 所示。

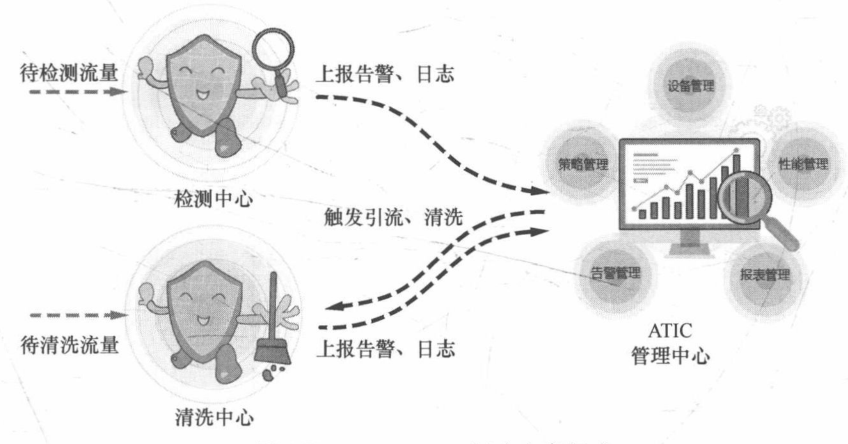


图 1-14　Anti-DDoS 解决方案组成

1. 检测中心

检测中心负责检测流量，发现攻击后上报管理中心，管理中心下发引流策略至清洗中心，清洗中心进行引流清洗。

2. 清洗中心

清洗中心主要根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。清洗中心提供多种 DDoS 流量清洗手段，可以准确识别正常流量，清洗各类异常流量，包括流量型攻击、应用层攻击、扫描窥探型攻击及畸形包攻击等。清洗中心同时具备检测中心的功能，当业务对检测清洗性能要求较低时可只部署清洗中心。

3. 管理中心

管理中心（Abnormal Traffic Inspection and Control System，ATIC）负责检测中心和清洗中心的统一管理，是 Anti-DDoS 解决方案的管理中枢。其具有设备管理、策略管理、性能管理、告警管理、报表管理等功能。

1.4.2 设备型号

Anti-DDoS 设备型号如图 1-15 所示。

高端设备

型号	AntiDDoS8030	AntiDDoS8080	AntiDDoS8160
检测中心	插检测业务板	插检测业务板	插检测业务板
清洗中心	插清洗业务板	插清洗业务板	插清洗业务板
说明	AntiDDoS8000是分布式设备，它的业务板类型决定设备类型。同时插检测和清洗业务板的设备称为混插设备，具备独立的检测和清洗功能		

中低端设备

型号	AntiDDoS 1520	AntiDDoS 1550	AntiDDoS 1500-D	AntiDDoS 1650	AntiDDoS 1680
检测中心	✗	✗	✓	✓	✓
清洗中心	✓	✓	✗	✓	✓
说明	AntiDDoS1500是集中式设备，它是清洗设备还是检测设备由设备型号决定			缺省情况下，AntiDDoS1600系列是清洗设备，可通过命令行切换为检测设备	

图 1-15 Anti-DDoS 设备型号

由图 1-15 可知，华为 Anti-DDoS 产品主要包括 AntiDDoS1000 和 AntiDDoS8000 系列，涵盖低、中、高端设备，型号齐全、功能丰富，可全方位满足用户各种需求。

1. AntiDDoS1500 系列产品介绍

在 AntiDDoS1500 系列产品中 AntiDDoS1500-D 为检测设备，AntiDDoS1520/AntiDDoS1550 为清洗设备。

2. AntiDDoS1600 系列产品介绍

AntiDDoS1600 系列产品使 AntiDDoS1000 系列产品摆脱了靠设备型号决定设备类型的规定，实现了通过命令行由清洗设备到检测设备的切换。

华为的 AntiDDoS1600 是企业级的 DDoS 防护系统，它可以针对中小型企业、政府、金融机构和 ICP 服务商的关键在线业务系统提供专业级防护方案。

3. AntiDDoS8000 系列产品介绍

AntiDDoS8000 系列具备全流量逐包检测、60 多种流量模型分析、全面的信誉体系、

T 级防护性能、秒级响应速度、100 多种攻击精准防护等功能。

1.4.3　方案部署位置

目前，Anti-DDoS 解决方案可以被广泛应用于运营商骨干网、城域网和企业网、IDC 等关键位置，可实现从骨干网到企业网的层层防护，如图 1-16 所示。下面我们具体介绍城域网、企业网和 IDC 的部署。

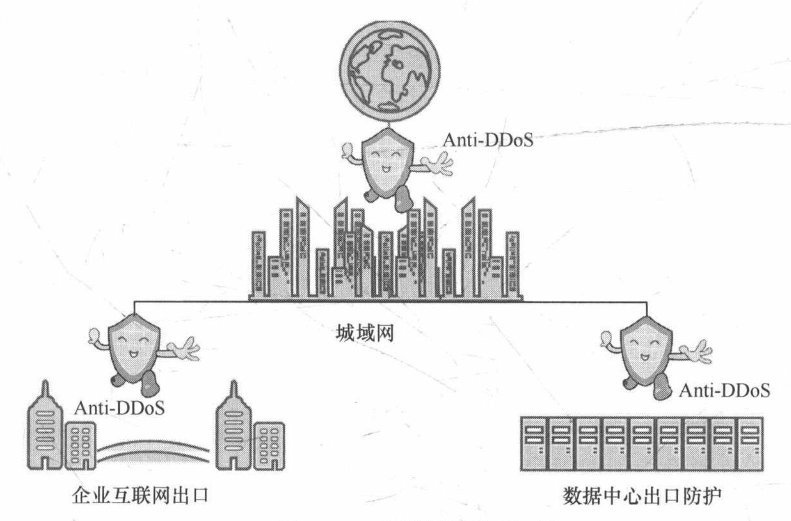


图 1-16　方案部署位置

1. 城域网部署

城域网部署可抵御外城域网对本城域网的 DDoS 攻击，保护城域网带宽资源可用。它可在防护对象汇聚处提供安全运营业务，提供增值服务，确保防护对象带宽资源及业务安全。

2. IDC 旁路部署

越来越多的企业业务和数据正从分散部署走向大集中，作为集中模式的代表，数据中心的出现极大地促进了企业的发展。IDC 出口带宽流量较大，业务类型丰富，对可靠性要求高，容易遭受泛洪类攻击和新型应用层攻击的双重威胁。Anti-DDoS 解决方案可确保托管服务器业务不中断，专业防护 HTTP、HTTPS、DNS、SIP Server，提供运营增值业务。

3. 企业网出口部署

企业网出口部署可帮助清洗从外部进入的 DDoS 攻击，防止内部主机服务器被黑客控制发起 DDoS 攻击。它对于业务流量模型的学习，可确保企业网带宽资源及应用业务服务器的安全。

1.4.4　方案部署模式

1. Anti-DDoS 设备部署模式

Anti-DDoS 方案主要支持直路部署、旁路静态引流和旁路动态引流部署三种模式，如图 1-17 所示。

（1）直路部署

直路部署组网简单，不需要额外增加接口。由于所有流量都将经过 DDoS 防护设备，

直路部署在个别攻击防护上要优于旁路部署。但这也是对 DDoS 防护设备可靠性的考验，因此，方案采取了清洗设备外置 Bypass 卡或直路双机的部署方式，保证系统在清洗设备故障时业务流量能够正常通过，增强链路可靠性。

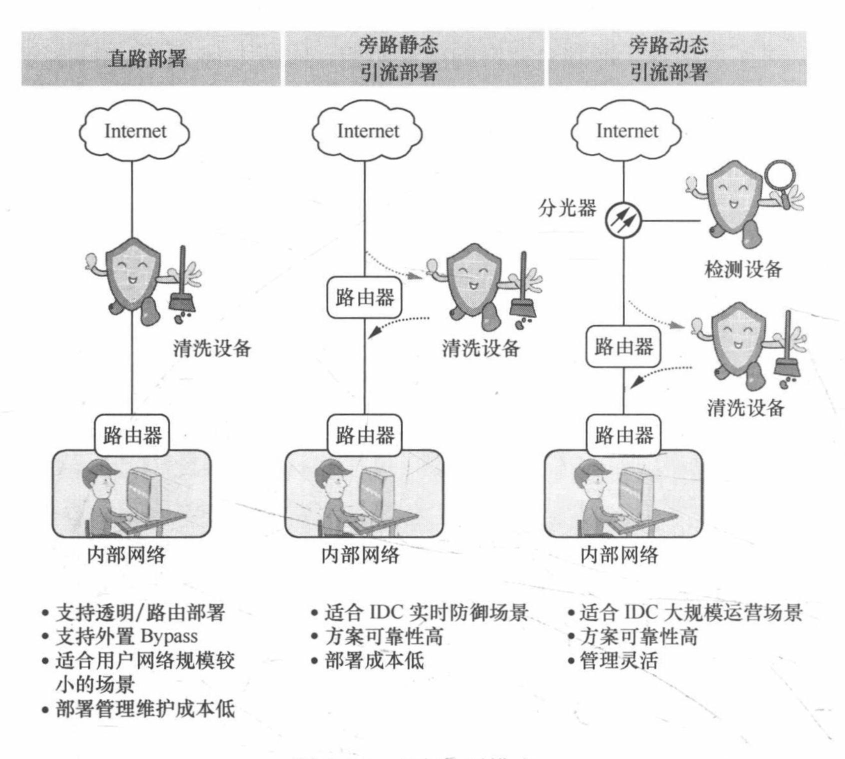


图 1-17 方案部署模式

这时，就出现了一个问题：如果用户组网复杂，难以使用直路部署，甚至不希望破坏原有组网，该怎么办？

（2）旁路静态引流部署

旁路部署应运而生，可完全解决上述问题。我们首先介绍旁路静态引流部署。所谓静态引流，就是将所有去往防护对象的流量都引流到清洗设备进行清洗，不论流量是否存在异常。这种方式虽然不用部署检测中心，但对清洗设备性能要求较高。如果清洗设备性能不足，有可能会影响客户的正常业务。

于是，又出现一个问题：在大流量场景下，如果 DDoS 防护设备处理所有流量将耗费大量的转发性能，导致安全投资上升，同时仍可能面临影响客户正常业务的风险。问题如何被彻底解决呢？

（3）旁路动态引流部署

动态引流部署应运而生，所谓动态引流，就是将去往防护对象的流量先复制一份到检测设备进行检测，如果发现存在异常流量才会被引流到清洗设备进行清洗。动态引流的优点在于只有异常流量才会被引流清洗，正常流量会被正常转发。

旁路动态引流部署在保证原有组网不被破坏的基础上，实现了上行流量无需经过 DDoS 防护设备，下行流量按需牵引的目标，使防护性能及可靠性都得到了保障。

2. ATIC 部署

在 Anti-DDoS 方案中，ATIC 的 Anti-DDoS 采集器和管理服务器支持分布式部署和集中式部署两种方式。

（1）集中式部署

Anti-DDoS 采集器和管理服务器同时被安装在同一台服务器上。集中式部署适用于 Anti-DDoS 设备都集中在一个局域网内的场景。

（2）分布式部署

Anti-DDoS 采集器和管理服务器被分别安装在不同服务器上，多台采集器可以共用一台 ATIC 服务器。分布式部署适用于 Anti-DDoS 设备分布在广域网各处的场景。

1.4.5　方案亮点

华为 Anti-DDoS 解决方案之所以能“脱颖而出”，是因为其具备以下亮点。

（1）响应快速

华为 Anti-DDoS 逐包检测方案响应时间为 2～3 秒，可保护业务永续无忧。

（2）性能高效

华为 AntiDDoS8000 系列具备单框最高 1440Gbit/s 的检测或清洗性能，整机性能较好。

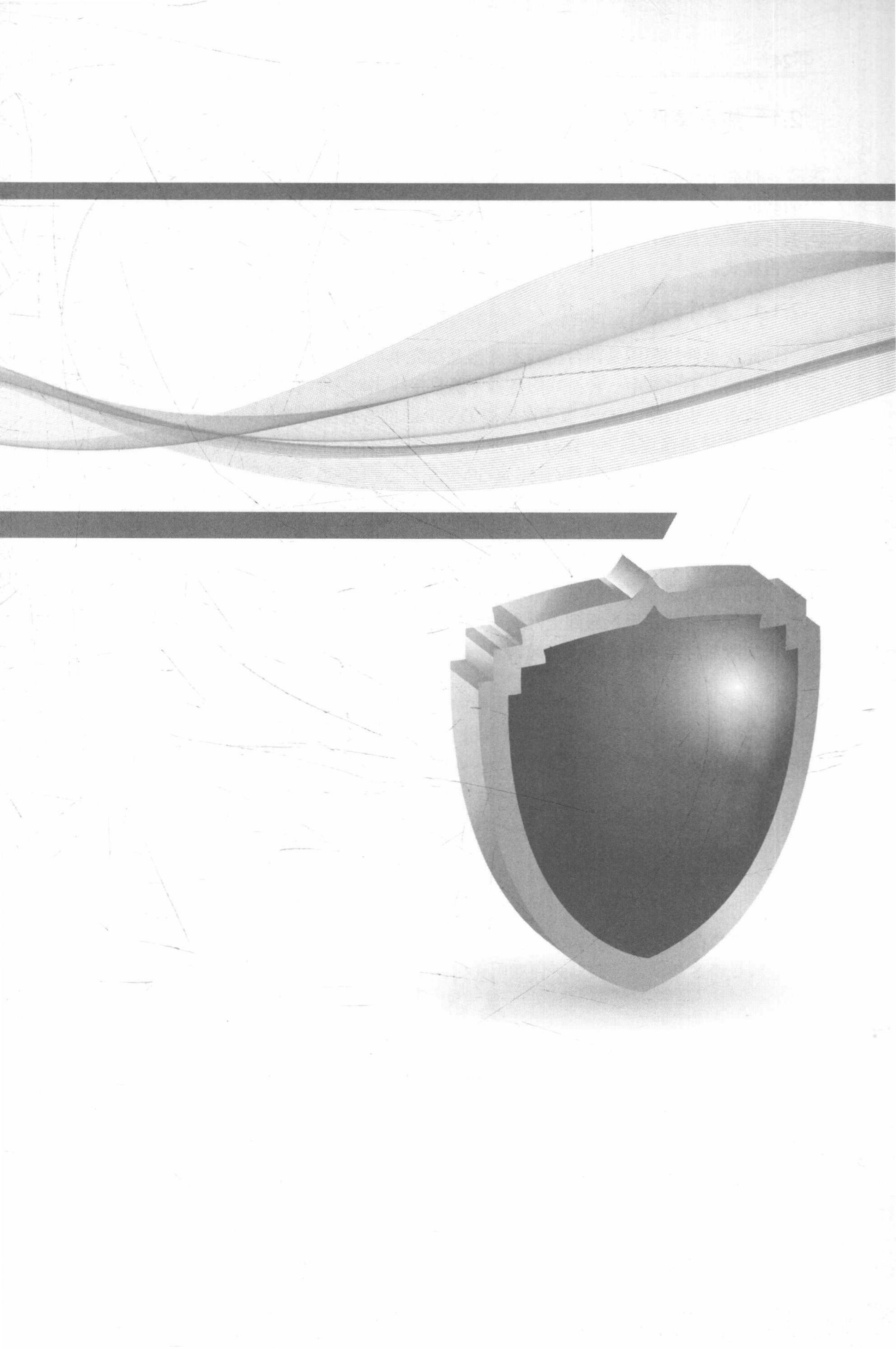
（3）防御精准

华为 Anti-DDoS 系统可精确防御 90%以上的流行 DDoS 攻击，防御种类 100 多种，比业界多 30%；率先支持 IPv6 防护，支持 IPv4/IPv6 双栈防护；多种技术保障零误判。

（4）增值运营

华为 Anti-DDoS 系统支持丰富的运营特性，运营商可以用其来为大客户提供 Anti-DDoS 防护增值业务；多样自助服务，丰富报表，可使企业对自身安全运营状态了如指掌；具有邮件、声音等多种告警模式，运维快速响应；多样化的客户自助服务，让客户的客户放心，增加客户黏度。

第2篇 DNS



2.1 热点事件解密之：视频软件断网事件

说到 DDoS 攻击，人们会不由自主地想起之前某视频软件（化名“龙卷风”）引发的断网事件。DDoS 攻击带来的巨大破坏使得短短两个小时内全国大部分地区的 DNS 服务器陆续瘫痪，导致用户不能正常上网，更为重要的是，众多黑客找到了一种新的攻击模式。

2.1.1 事件回顾

此次事件的起因是两台游戏服务器互相竞争，来回发动 DDoS 攻击。在达不到预期效果的情况下，其中一台游戏服务器干脆直接攻击对方的域名服务器。

攻击发生当晚，DNS 服务提供商 DNSPod 的 6 台服务器开始受到攻击。当晚 20 点 33 分，在大流量攻击下，DNSPod 的 6 台服务器开始陆续失效，大量网站开始间歇性无法访问。第一波攻击的流量在 21 点 30 分左右达到高峰，流量超过了 10Gbit/s。此时，由于 DNSPod 耗尽了整个机房近乎三分之一的带宽资源，为了不影响机房其他用户使用，DNSPod 服务器被运营商下线。

如果事情到此为止，其实也不会造成多大的影响。可是，DNSPod 并不仅仅为这个被攻击的游戏服务器提供域名解析服务，它还支持数十万其他的网站，这其中就包括“龙卷风”软件。普通用户遇到上网失败时，尝试几次就放弃了；可这个软件的设计使它在请求失败后持续不断地重新发起请求，攻击如图 2-1 所示。

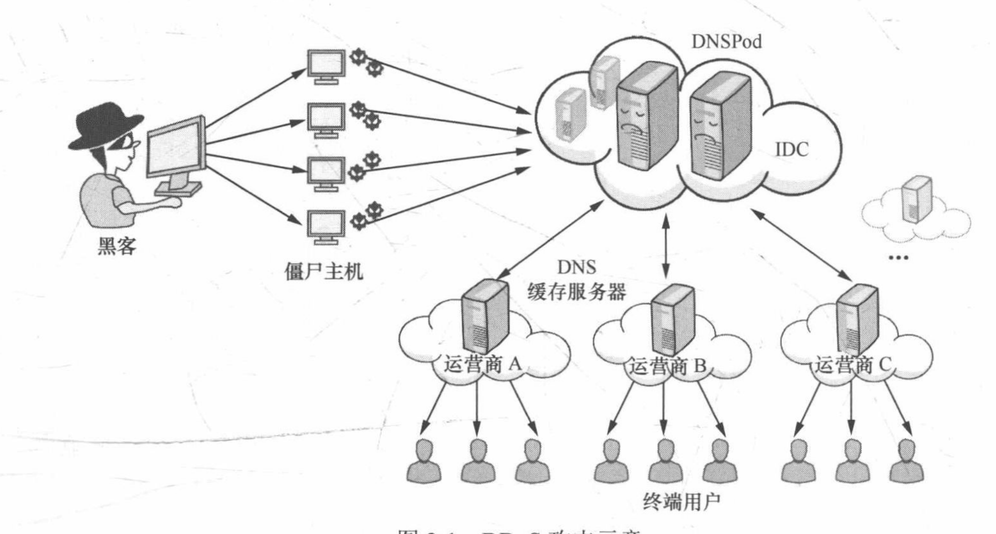


图 2-1 DDoS 攻击示意

攻击发生的第二天晚上，由于 DNSPod 网络服务被中断，致使其无法提供域名解析服务。诸多采用 DNSPod 服务的网站无法被访问，DNS 请求涌向了本地 DNS 缓存服务器，DNS 缓存服务发生了大面积的堵塞情况。之后的两个小时内全国大部分地区的 DNS 缓存服务器开始陆续瘫痪，全国出现大面积断网情况。

2.1.2　事件中涉及的几个关键角色

① DNSPod：国内最大的一家免费 DNS 服务提供商，“龙卷风”软件和前面恶性竞争的游戏服务器都是 DNSPod 的客户。

② 运营商：DNSPod 无法独立承建数据中心，只能租用运营商 IDC 的机房和服务器资源。

③“龙卷风”软件：软件中有一项强制随机启动的进程，只要用户安装了该软件，该进程就会自动运行，并不断连接视频网站，下载广告或升级软件。

整个事件有以下几个关键点。

① 游戏服务器攻击竞争对手的 DNS 服务，间接攻击了整个 DNSPod 的业务。

② 运营商阻断了 DNSPod 流量，粗暴地对流量进行了黑洞处理。

③ 几亿台安装了“龙卷风”客户端的 PC 充当“肉鸡”，导致运营商 DNS 缓存服务器无法提供服务，进而导致大面积断网。

如果我们把这次事件看成是“多米诺骨牌”效应，那被推倒的第一张“骨牌”是 DNSPod 服务器；第二张“骨牌”毫无疑问就是“龙卷风”软件，该软件充当“肉鸡”角色导致服务器耗尽了电信运营商 DNS 缓存服务器；而第三张“骨牌”就是全国范围瘫痪的网络了。如果我们想深入理解这次互联网灾难，要先从 DNS 的基础知识讲起。

2.1.3　DNS 服务器在网络中充当的角色

大家都知道，我们在上网的时候，输入的网址其实是一个域名。

网络上的计算机彼此之间只能用 IP 地址相互识别，但是 IP 地址是一串数字，很难被记忆，所以域名便出现了。域名很容易被人们记住，我们在上网的时候可以直接输入域名，计算机需要通过域名找到对应的 IP 地址，这就是域名解析的过程。

域名解析要由专门的域名解析系统（Domain Name System，DNS）来完成。如图 2-2 所示，DNS 中涉及以下几种类型的服务器。

1. 根服务器

根服务器主要管理互联网的主目录。全世界只有 13 个根逻辑服务器节点。这 13 个节点中有 10 个被部署在美国，剩下 3 个分别位于英国、瑞典和日本。虽然网络是无国界的，但服务器是有国界的。所有根服务器均由美国政府授权的互联网域名与号码分配机构 ICANN 统一管理。

2. 顶级域名服务器

顶级域名服务器一般存储.com、.edu、.cn 等顶级域名。

3. 递归服务器

递归服务器也可被理解为存储官方域名解析授权的授权服务器，它一般存储着网络中域名和 IP 地址的解析关系，也就是 DNSPod 充当的角色。试想一下，如果每个上网用户在上网的时候都向授权服务器发送请求，那授权服务器可能无法承受如此大的请求数量，因此，缓存服务器的存在是有必要的。

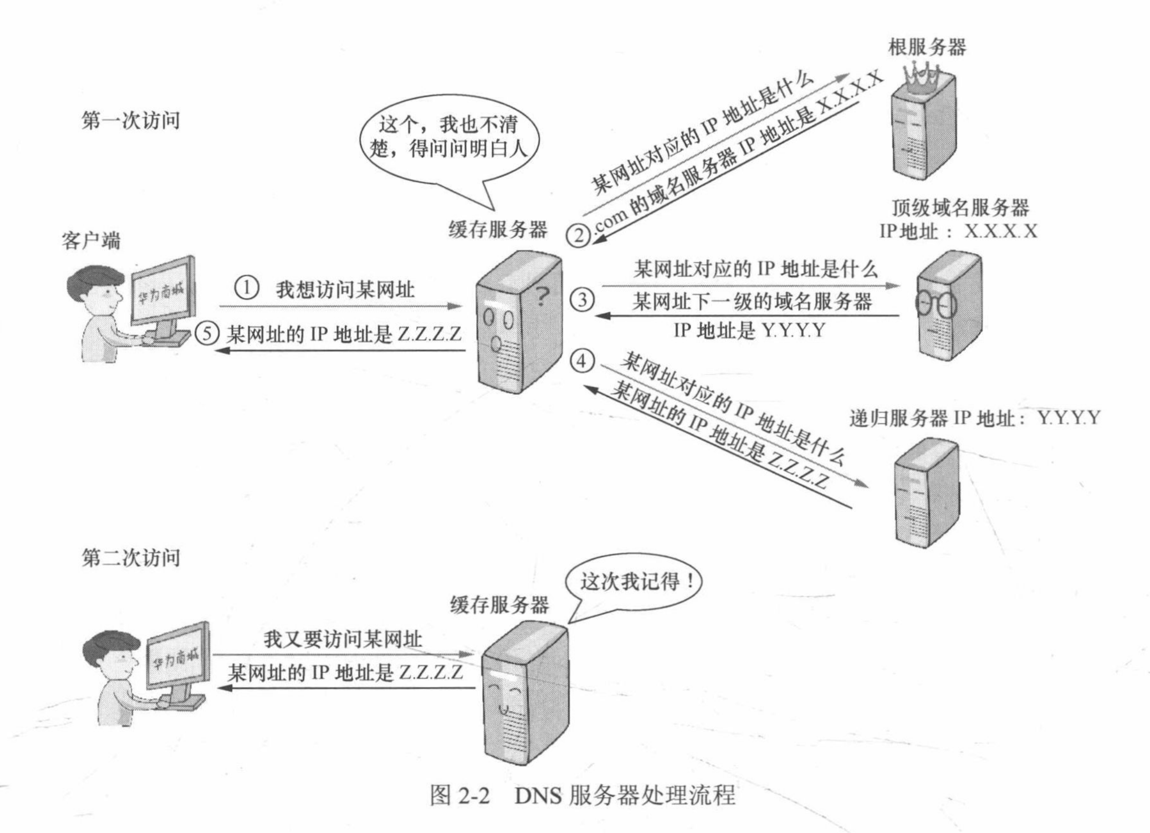


图 2-2 DNS 服务器处理流程

4. 缓存服务器

缓存服务器相当于授权服务器的一个代理，可以缓解授权服务器的压力。我们每次上网的时候，域名解析的请求都被发给缓存服务器了。缓存服务器第一次收到用户请求的时候，会向授权服务器请求域名和 IP 地址的解析表，然后将其储存到本地，等后续再有用户请求相同的域名时，就会直接答复，不再向授权服务器请求，毕竟一个网站的 IP 地址不是经常变化的。当然，这个解析表是有一定有效期的，等有效期到了，这个解析表就会自动老化，下次有用户请求时缓存服务器就会重新询问授权服务器。这个定期老化机制可以保证缓存服务器上的域名解析能定期更新。

① DNS 客户端查询通常采用递归方式，缓存服务器首先会判断本地是否有这个域名的解析缓存。

② 如果本地没有该域名的解析缓存，缓存服务器就会把域名发送到根服务器。根服务器收到某网址的请求后，会判断.com 是由谁授权管理的，并返回.com 所在的顶级域名服务器 IP 地址。

③ 缓存服务器继续向顶级域名服务器发送某网址解析请求，顶级域名服务器收到请求后，会返回某网址下一级的递归服务器 IP 地址。

④ 缓存服务器继续向递归服务器发送某网址解析请求，递归服务器收到请求后，返回某网址的解析 IP 地址。如果域名层级较多，递归服务器层级也会越多。

⑤ 缓存服务器得到某网址的解析 IP 地址后，将 IP 地址发送给客户端，同时在本地缓存。

⑥ 后续一段时间内，当有客户端再次请求某网址的域名解析时，缓存服务器直接回应解析的 IP 地址，不再重复询问。

2.1.4　针对关键环节的解决方案思路

我们继续回到“龙卷风”软件这件事上。在当年，运营商对 DNSPod 采用的是粗暴式的黑洞处理，显然这种方式是不合适的，其直接影响了其他域名的解析业务。

DNS 递归（授权）服务缺少有效的保护，运营商 IDC 和 SP 缺少应用层清洗能力，无法识别应用层的攻击流量针对性地清洗攻击流量。

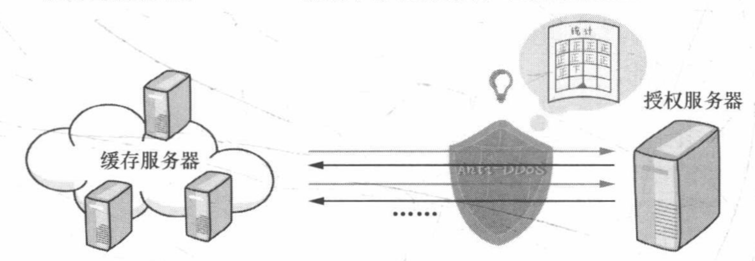
2.1.5　华为 Anti-DDoS 系统的解决方案

华为 Anti-DDoS 专业防御系统对 DNS 服务器提供精细化的防御。精细化的意思是针对不同的 DNS 服务器、不同的攻击类型、不同的应用场景，该系统会提供不同的防御手段。华为 Anti-DDoS 针对这次事件可以从两方面进行部署。

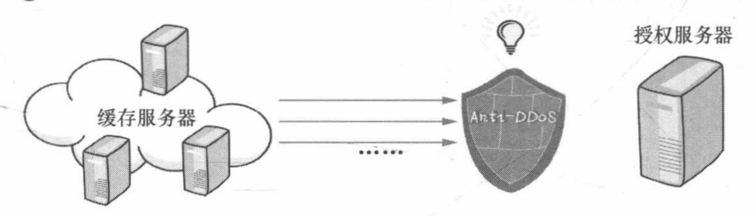
1. 授权服务器防护

DNSPod 服务器的防护可以作为第一道防线。由于 DNSPod 服务器所遭受的攻击其实都是僵尸主机发送的 DNS 请求，属于虚假源攻击，所以它可以采用重定向方式进行防御，如图 2-3 所示。

① Anti-DDoS 系统被部署在授权服务器前，统计到达授权服务器的流量。流量达到告警阈值前，Anti-DDoS 系统只对其进行统计，不进行其他处理



② 流量达到告警阈值后，Anti-DDoS 系统启动源认证，重定向请求报文



③ 如果是真实存在的源，Anti-DDoS 系统会正常响应源认证报文

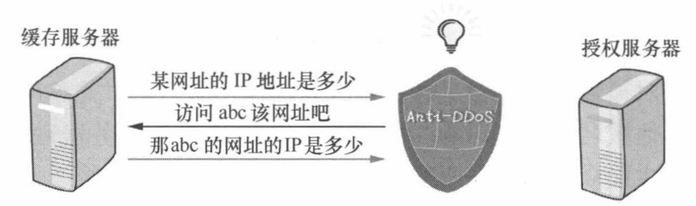


图 2-3　授权服务器源认证

④ 认证通过的源，Anti-DDoS 系统会将此源记录到白名单中，后续这个源发送的请求将被直接通过，不需重复认证

真实缓存服务器

授权服务器

还就继续访问某网址吧

某网址的 IP 是多少

Anti-DDoS

某网址的 IP 是 Z.Z.Z.Z

⑤ 如果是虚假源，Anti-DDoS 系统不会正常响应源认证报文，所有它发送的请求报文也不会到达授权服务器。

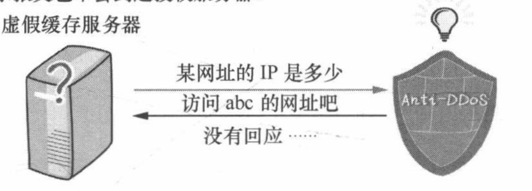


图 2-3　授权服务器源认证（续）

2. 缓存服务器防护

如果 DNSPod 服务器不幸失效了，那我们还可以通过保护 DNS 缓存服务器来对其进行保护，这是阻止事件继续恶化的第二道防线。

DNS 缓存服务器和 DNSPod 服务器所遭受的攻击不同，毕竟“龙卷风”软件的用户都是真实存在的源，这种攻击属于真实源攻击。源认证防御方式对这种真实源攻击无效，所以我们可以采用以下应对方法。

首先，Anti-DDoS 系统支持针对 DNS 服务的 Top N 统计，并提供报表。如图 2-4 所示。从报表中，我们可以获知访问最多的 Top N 域名，在这么大的访问量下，“龙卷风”软件一定是名列前茅的。

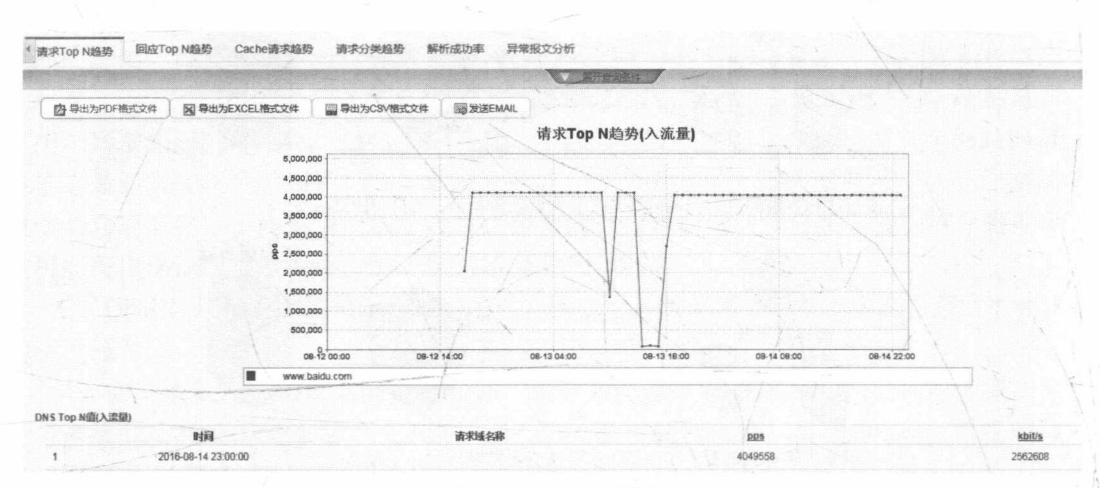


图 2-4　Top N 统计

然后，我们对被攻击的域名进行指定域名限速，即限速“龙卷风”软件的域名。这样就可以避免其他域名服务受影响，也不会导致 DNS 缓存服务器瘫痪。

域名作为广大民众访问互联网的起点和入口，是全球互联网通信的基础。域名解析系统作为承载全球亿万域名正常使用的系统，是互联网的基础设施。而域名系统又是一种公开服务，很容易成为被黑客攻击的对象。域名系统的故障会导致互联网陷入瘫痪，

所以域名系统的保护也变得至关重要。

“龙卷风”软件攻击事件的第二阶段，也就是DNS缓存服务器拒绝服务，导致大面积Internet接入瘫痪的过程，才是本次攻击的“威力点”。这个结果虽然不是攻击者的本意，但是一连串的连锁反应，使它成为DDoS攻击史上具有里程碑意义的关键事件。它给了DDoS攻击者新的方向，使其知道了如何利用庞大的网络基础设施架构制造更强大、更真实的DDoS攻击。后面的NTP反射攻击，视频签名嵌入式攻击等都是源于这个思路，此次事件是DDoS发展的里程碑事件。

2.2　DNS协议解析

近几年，DNS攻击成为应用层DDoS攻击的代表性攻击，其每年发生的频率都在大幅上升，DNS攻击造成的影响也非常大。

2.2.1　DNS协议基础

想要理解DNS攻击的原理，我们就要先明白DNS协议的基础，我们从DNS协议本身来进行介绍。DNS通过RFC1034、1035协议定义规范，属于应用层协议。在前文中，我们也提到，DNS是互联网上非常重要的一项服务，我们每天上网都要依靠大量的DNS服务。在Internet上，用户更容易记住的是域名，但是网络中的计算机的互相访问是通过IP地址实现的。DNS最常用的功能是给用户提供域名解析服务，将用户的域名解析成网络上能够访问的IP地址。

下面我们来研究DNS报文的格式。

2.2.2　DNS报文格式

DNS报文格式如图2-5所示。



图2-5　DNS报文格式

下面我们结合 DNS 查询报文和响应报文的抓包信息来理解报文格式中的几个关键字段，我们先了解一下 DNS 查询报文的抓包，如图 2-6 所示。

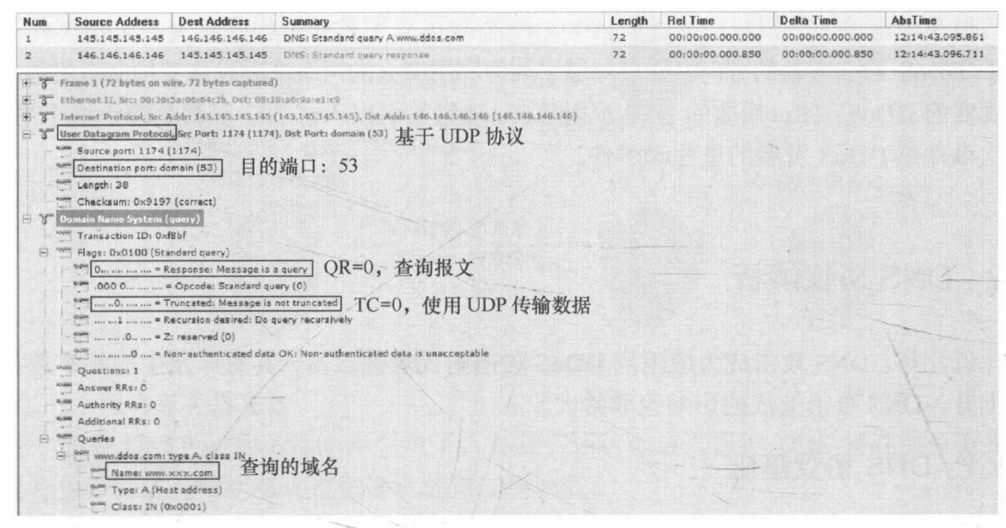


图 2-6 DNS 查询报文抓包

DNS 报文由 12B 长的首部和 4 个长度可变的字段组成。标识字段由客户端程序设置并由服务器返回结果，客户端通过标识来确定响应与查询是否匹配。报文中涉及的字段很多，我们重点解释以下几个关键字段。

① UDP：DNS 查询是基于 UDP 传输数据的。DNS 服务器支持 TCP 和 UDP 两种协议的查询方式。

② Destination port：目的端口默认是 53。

③ QR：0 表示查询报文；1 表示回应报文。

④ TC：表示“可截断”。使用 UDP 时，当应答报文超过 512Byte 时，只返回前 512Byte。

通常情况下，DNS 查询都是使用 UDP，UDP 提供无连接服务器，查询速度快，可降低服务器的负载。当客户端发送 DNS 请求，并且返回响应中 TC 位设置为 1 时，就意味着响应的长度超过 512Byte，而仅返回前 512 个字节。这种情况下，客户端通常采用 TCP 重发，将重发原来的查询请求，并允许返回的响应报文超过 512Byte。简单来说，就是 UDP 报文的最大长度为 512Byte，而 TCP 则允许报文长度超过 512Byte。当 DNS 查询超过 512Byte 时，协议的 TC 标志位会被置为 1，这时则使用 TCP 发送。

⑤ Queries：表示 DNS 请求的域名和类型。

接下来我们再来了解 DNS 回应报文的抓包，如图 2-7 所示。回应报文比查询报文多了后 3 个字段：回答字段、授权字段和附加信息字段。其中回答字段放置的是域名对应的 IP 地址等信息。

① Name：DNS 查询中的请求域名。

② Type：每一个查询都有一个查询类型，每一个响应也都有一个响应类型。这个类

型大约有 20 多种，但是很多现在已经过时了。最常用的查询类型是 A 类型，它表示期望获得查询域名的 IP 地址。查询类型也可以是 CNAME。

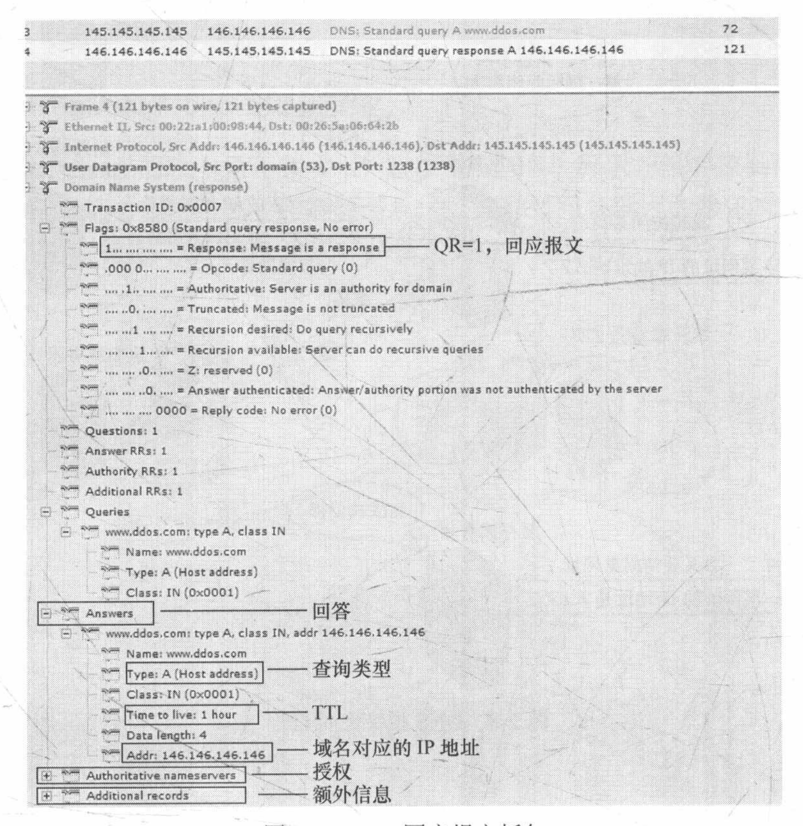


图 2-7 DNS 回应报文抓包

③ TTL：生存时间，表示客户端保留该解析资源记录的时间。

2.2.3 DNS 交互

假设一个用户要去华为商城买一部手机，那么从他在浏览器上输入华为商城的域名，到打开商城网页的一瞬间，其实发出的 DNS 请求报文已经经历了图 2-8 所示的查询过程。

为了便于理解，我们简化一下 DNS 报文交互的流程，如图 2-9 所示。递归服务器这种有官方域名授权的服务器，我们暂且把这类服务器统一归类为“授权服务器”。这样 DNS 服务就可以被分为两大类：一种是授权存储域名和 IP 地址映射关系的授权服务；另一种是临时存放域名和 IP 地址映射关系的缓存服务。

DNS 查询通常都是基于 UDP 的，这就导致了在查询过程中验证机制的缺失，黑客很容易利用该漏洞进行分析。下面，我们就分析一下这两类服务可能面临的 DNS 攻击风险。

风险一，黑客伪造客户端源 IP 地址发送大量的 DNS 请求报文，造成 DNS request flood 攻击。DNS request flood 是当前最常见的 DNS 攻击。这类攻击可以针对缓存服务

器，也可以针对授权服务器。

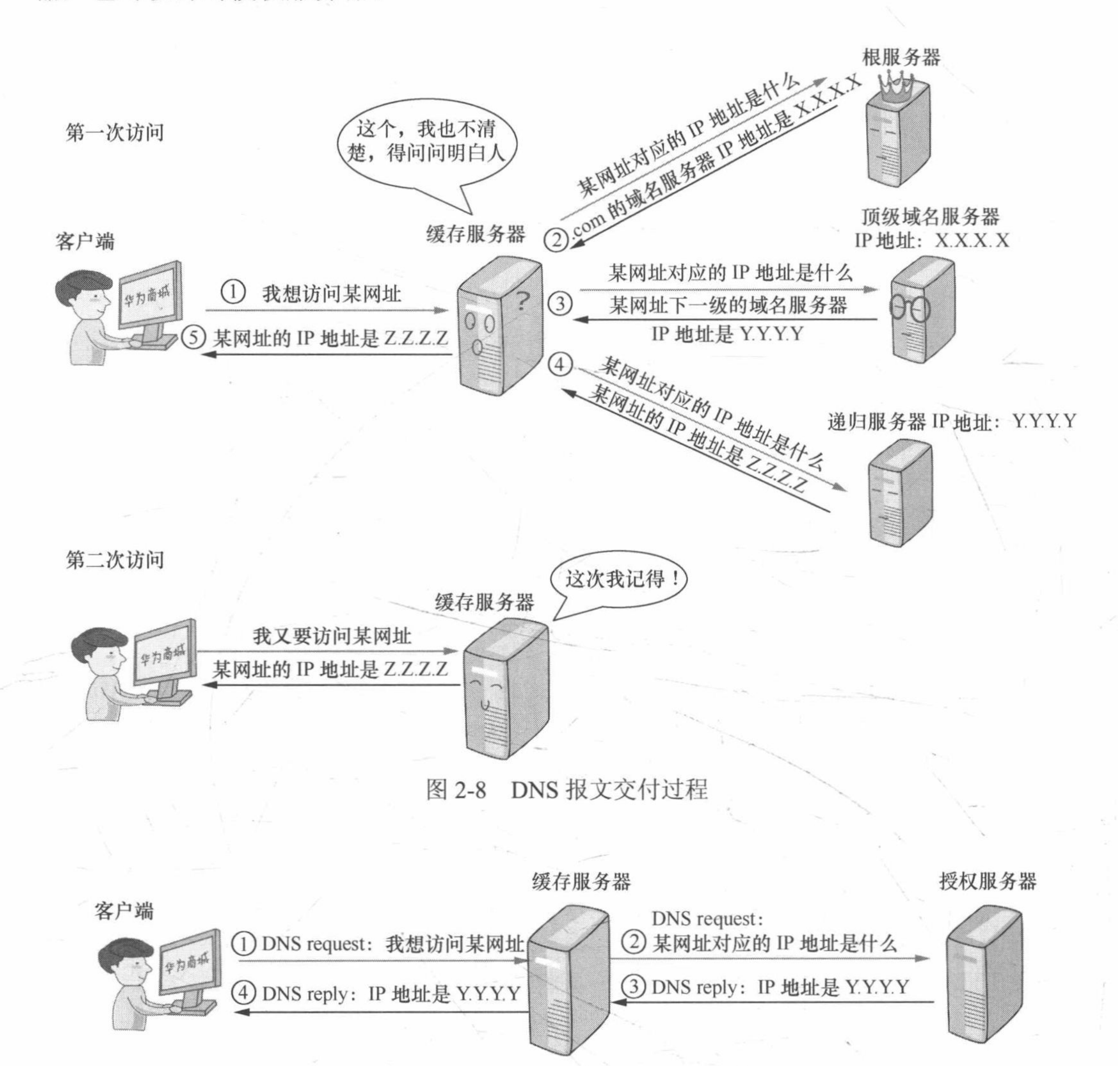


图 2-8 DNS 报文交付过程

图 2-9 DNS 报文交付简化过程

风险二，黑客伪造成授权服务器发送大量的 DNS 回应报文，造成 DNS reply flood 攻击。

风险三，黑客篡改某些网站的域名和 IP 地址对应关系，导致用户访问被导向至其他网站。

风险四，黑客向 DNS 服务器发送大量错误格式的 DNS 异常报文，或者发送大量超长 DNS 报文，导致 DNS 服务器处理这些报文时出现异常，拒绝正常服务。

当然，DNS 的查询过程主要是基于 UDP 的，也有少量基于 TCP，所以除了应用层攻击外，其可能也会遭受传输层的 TCP 或 UDP 类攻击，比如 SYN flood、UDP flood 等。

在“龙卷风”软件案例中，我们介绍了一些和案例本身相关的 DNS 攻击，以及适合此场景的防御措施。其实 DNS 的攻击和防御措施远不止这些，接下来我们就重点介绍安全领域比较常见的一些 DNS 攻击以及相应的防御措施。

2.3 DNS Request Flood 攻击与防御

2.3.1 DNS Request Flood 攻击原理

DNS request flood 的攻击原理其实很简单，如图 2-10 所示。黑客控制僵尸网络向 DNS 服务器发送大量不存在的域名的解析请求，最终导致服务器因大量 DNS 请求而超载，无法继续响应正常用户的 DNS 请求，从而达到攻击的目的。

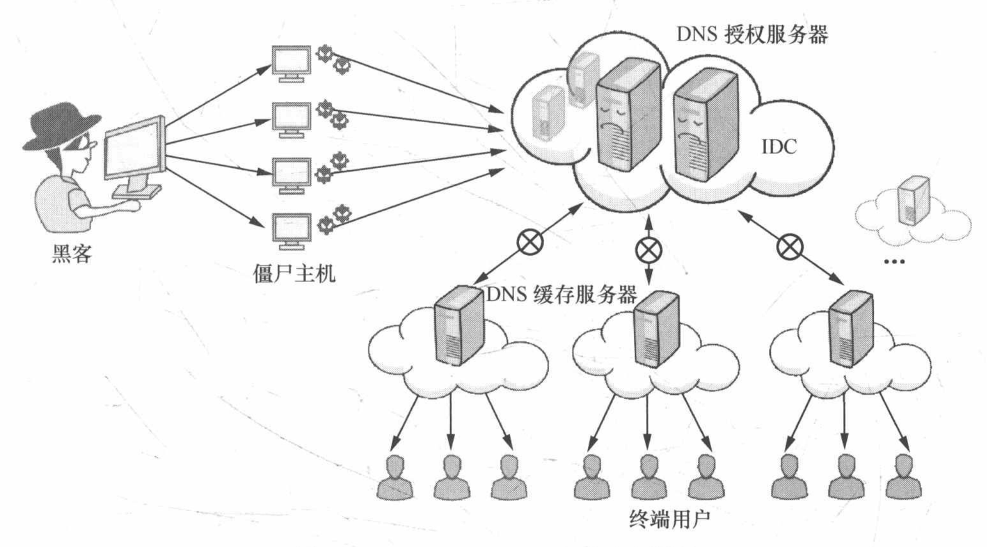


图 2-10 DNS request flood 的攻击原理

在 DNS request flood 的攻击过程中，黑客的攻击目标可能是 DNS 授权服务器，也可能是 DNS 缓存服务器。黑客伪造的客户端 IP 地址可能是虚假源 IP 地址，也可能是现网真实存在的 IP 地址。如果遭受攻击的是 DNS 授权服务器，大量不存在的域名解析请求会导致服务器应接不暇，最终导致服务器性能耗尽；如果遭受攻击的是缓存服务器，则会导致缓存服务器不停地向授权服务器发送这些不存在的域名的解析请求，一收一发更加重服务器的负担，直到导致服务器瘫痪。

对于缓存服务器和授权服务器，虽然遭受的都是 DNS request flood 攻击，但由于请求的客户端类型不同，所以其防御的手段也不同。对于缓存服务器，正常向它发送 DNS 请求的是上网的终端用户，所以在防御过程中，其需要先判定这个 DNS 请求是否由真实、正常的浏览器客户端发出；而对于授权服务器，正常情况下与其交互的是缓存服务器，所以向它发送 DNS 请求的可能就是缓存服务器。因此对于不同的对象，认证方式当然也不同了。

2.3.2 华为 Anti-DDoS 系统如何防御 DNS Request Flood 攻击

我们先从缓存服务器讲起，看看华为 Anti-DdoS 系统是怎么防御 DNS request

flood 攻击的。Anti-DDoS 系统防御 DNS request flood 攻击最初采用的方式是 TC 源认证方式。

1. TC 源认证

DNS 查询有 TCP 和 UDP 两种方式。通常情况下，DNS 查询都是基于 UDP 的，此时 TC 标志位置为 0，其可以通过将 TC 标志位置为 1 来将 UDP 改为 TCP 方式。华为 Anti-DDoS 系统就是通过修改 DNS 报文中的 TC 标志位，对客户端进行源认证的，如图 2-11 所示。

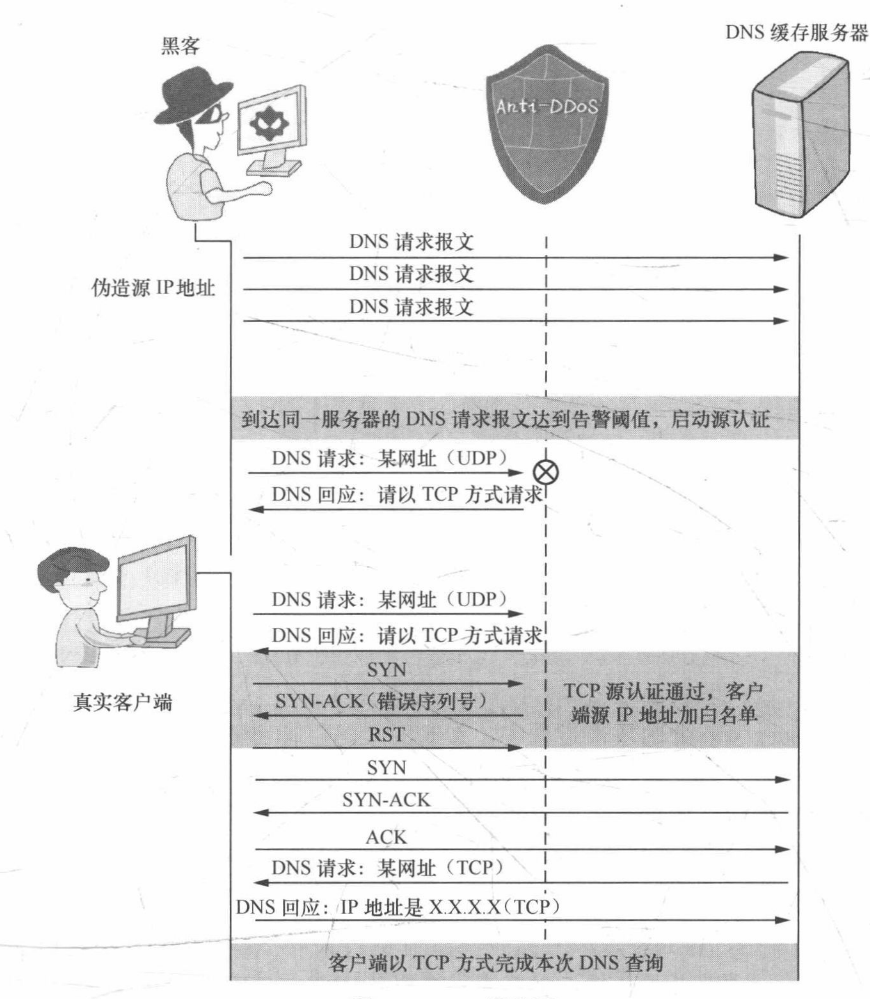


图 2-11 TC 源认证

TC 源认证交互过程如下。

① 当客户端发送的 DNS 请求报文长度超过告警阈值后，Anti-DDoS 系统启动源认证机制。

② Anti-DDoS 系统拦截 DNS 请求，将 TC 标志位置为 1 并进行回应，要求客户端以 TCP 方式重新发起 DNS 查询。

③ 如果这个源是虚假源，则 Anti-DDoS 系统不会正常响应这个 DNS 回应报文，更不会通过 TCP 方式重新进行 DNS 查询。

④ 如果是真实客户端发送的请求，则 Anti-DDoS 系统会重新发送 SYN 报文，请求建立 3 次握手。

⑤ Anti-DDoS 系统对客户端源进行 TCP 层面的认证。源认证通过后，客户端源 IP 地址被加入白名单。

⑥ 客户端重新请求建立 3 次握手，Anti-DDoS 系统将客户端第 2 次发送的 3 次握手请求直接放行，发送给服务器。

⑦ 客户端与服务器之间建立 3 次握手成功，并通过 TCP 方式完成本次 DNS 查询。

我们再来结合一组抓包深入了解此过程。

① 客户端向 DNS 服务器第一次发送 DNS 请求报文，从图 2-12 所示的抓包中可以看出，DNS 请求报文基于 UDP，TC 标志位是 0，请求的域名是 www.×××.com。

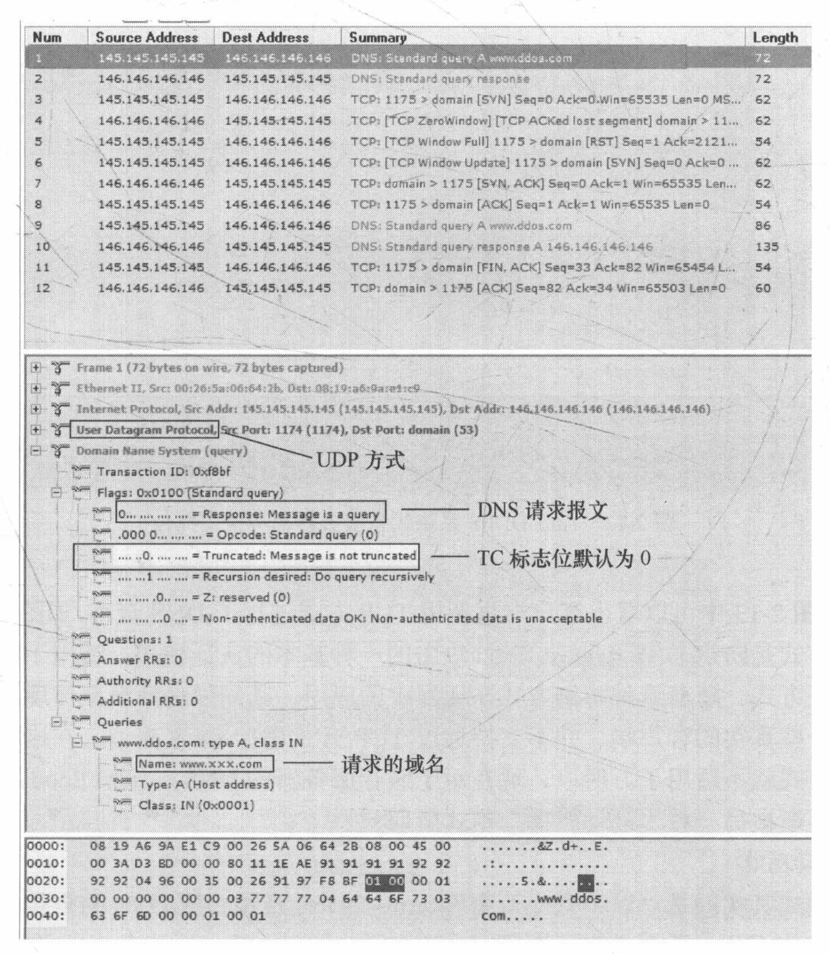


图 2-12 客户端第一次发送 DNS 请求抓包

② Anti-DDoS 系统代替 Web 服务器进行回应，并将 TC 标志位设置为 1，希望客户

端通过 TCP 方式重新发起 DNS 查询，如图 2-13 所示。

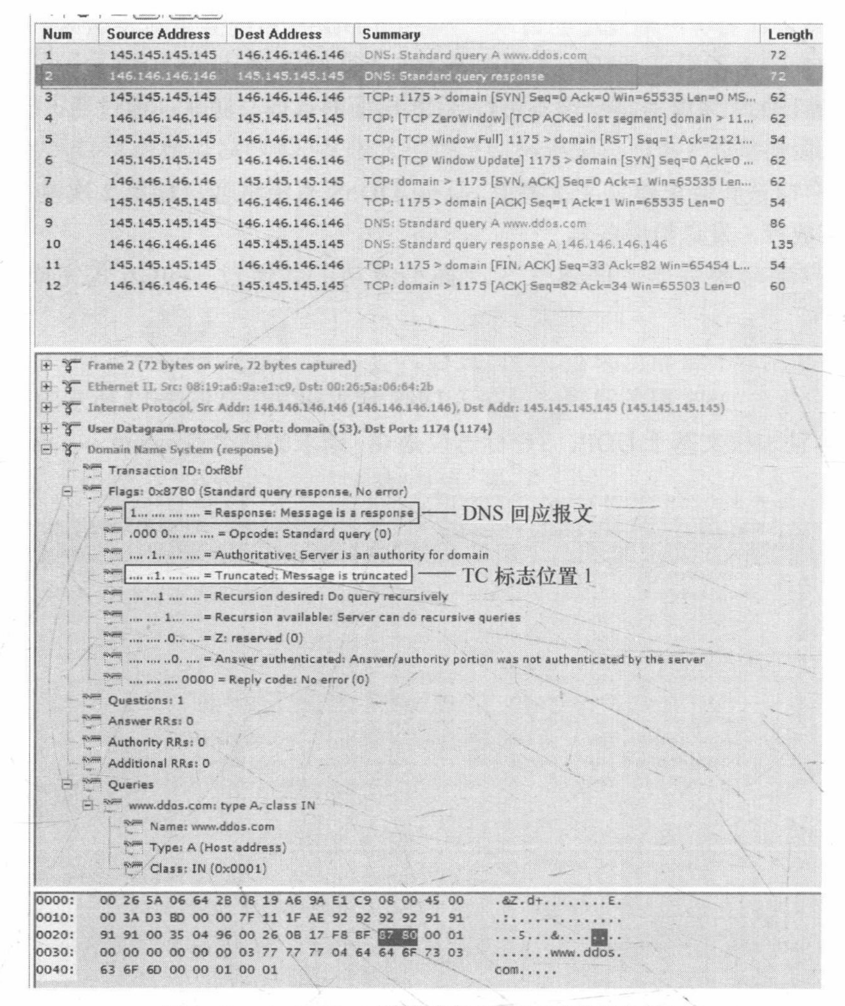


图 2-13　Anti-DDoS 系统代替服务器回应报文抓包

③ 从图 2-13 中可以看出客户端重新用 TCP 方式进行了 DNS 查询，如图 2-14 所示。

这种方式是防御 DNS request flood 攻击的一种基本的认证模式，适用于客户端是浏览器的认证方式。随着这种防御方式在现网中的应用，其局限也渐渐地显现出来。比如现网中有一些真实的客户端，并不支持通过 TCP 方式进行 DNS 查询，在这种情况下，这种防御方式就不适用了。所以，现在对于缓存服务器的 DNS request flood 攻击的防御模式已经逐渐被另一种“被动防御”模式所取代。

2. *被动防御*

被动模式其实就是“以不变应万变”，Anti-DDoS 系统利用 DNS 的重传机制，不反弹 DNS 查询报文，而是直接不处置，将其丢弃，然后看客户端是否重传，如图 2-15 所示。

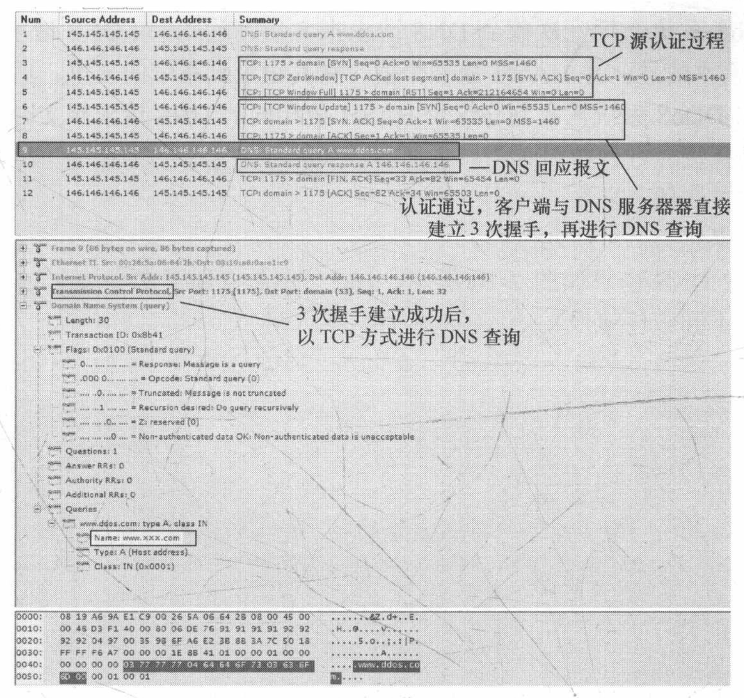


图 2-14 客户端重新用 TCP 方式进行 DNS 查询抓包

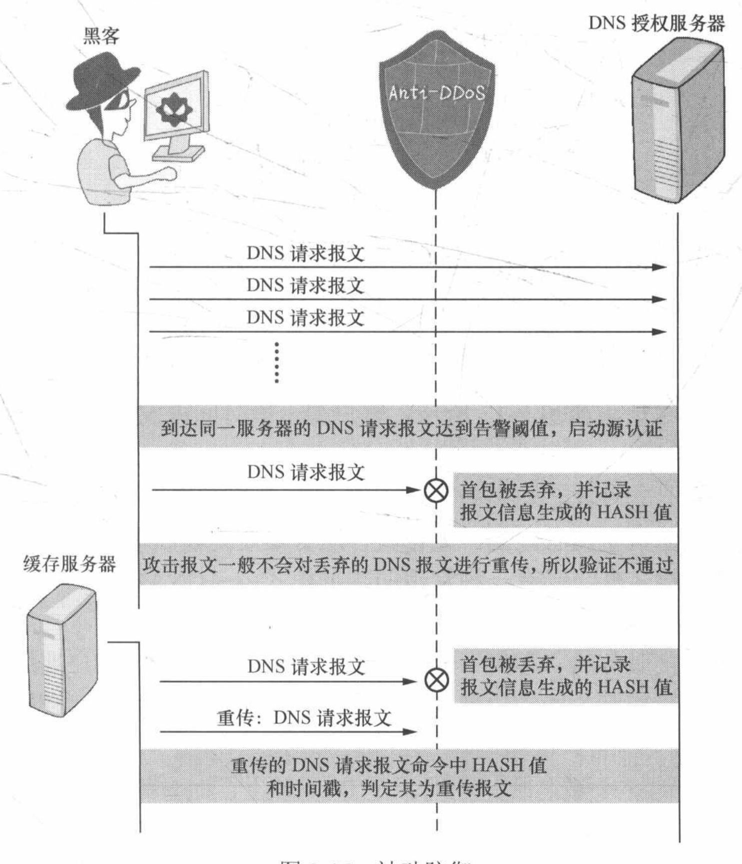


图 2-15 被动防御

Anti-DDoS 系统在第一次收到 DNS 请求报文后，就会记录 DNS 请求报文的域名、源 IP 地址等基本信息，并 HASH 成一个值，将其记录到系统的表里。后续一定时间戳内，如果 Anti-DDoS 系统再收到与这个 HASH 值相同的 DNS 请求报文时，就认定其为重传包，对其执行放行操作。时间戳会随着收到的每一个相同 HASH 值的 DNS 请求报文包而不断地被刷新。

我们再以抓包为例了解此过程。

① 第一次 DNS 请求如图 2-16 所示。这个 DNS 查询报文会被 Anti-DDoS 系统丢弃，并且系统不回应任何报文。

图 2-16 第一次 DNS 请求抓包

② 第二次 DNS 请求如图 2-17 所示。客户端一段时间内没有收到 DNS 回应报文，重新发送 DNS 请求报文。

被动防御模式是一种比较通用的防御手段，适用于攻击源不断变换的 DNS 请求攻击，但其对客户端的类型没有限制，无论缓存服务器还是授权服务器都适用。对于授权服务器，除了被动模式外，还有一种常用的防御模式——CNAME。

3. CNAME 模式

授权服务器直接服务的“客户”通常是缓存服务器，而不是客户端的浏览器。所以在源认证的时候，授权服务器的防御机制和缓存服务器的机制不同。授权服务器利用的是 DNS 的 CNAME（别名）机制。

DNS 协议允许将多个域名映射到同一个 IP 地址上，此时可以将一个域名作为 A 记录指向服务器 IP 地址，然后将其他域名作为别名，指向之前有 A 记录的域名。这样类型的存在是为了保证在 IP 地址变更时，系统不必一个一个地对域名做出相应更改指向。

应用此种机制后，系统只需要更改 A 记录的相应域名到新 IP 地址上，其他别名将自动被更改到新 IP 地址上。

Num	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
1	145.145.145.145	146.146.146.146	DNS: Standard query A www.ddos.com	72	00:00:00.000.000	00:00:00.000.000	14:10:02.237.855
2	145.145.145.145	146.146.146.146	DNS: Standard query A www.ddos.com	72	00:00:04.993.625	00:00:04.993.625	14:10:07.231.480
3	146.146.146.146	145.145.145.145	DNS: Standard query response A 146.146.146.146	121	00:00:05.023.755	00:00:00.030.130	14:10:07.261.610

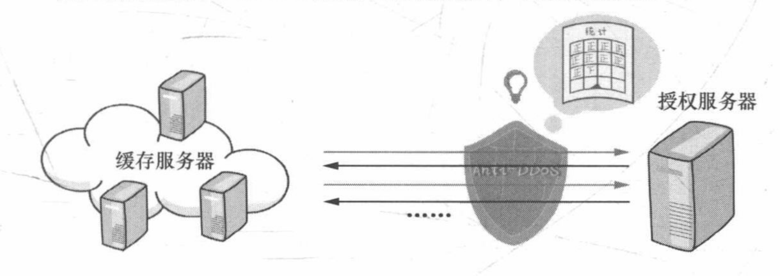
```
Frame 2 (72 bytes on wire, 72 bytes captured)
Ethernet II, Src: 00:26:5a:06:64:2b, Dst: 08:19:a6:9a:e1:c9
Internet Protocol, Src Addr: 145.145.145.145 (145.145.145.145), Dst Addr: 146.146.146.146 (146.146.146.146)
User Datagram Protocol, Src Port: 1182 (1182), Dst Port: domain (53)
Domain Name System (query)
    Transaction ID: 0xf21d
    Flags: 0x0100 (Standard query)
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ddos.com: type A, class IN
            Name: www.XXX.com
            Type: A (Host address)
            Class: IN (0x0001)

0000:  08 19 A6 9A E1 C9 00 26 5A 06 64 2B 08 00 45 00   .......&Z.d+..E.
0010:  00 3A 0B 7A 00 00 80 11 E6 F1 91 91 91 91 92 92   .:.z............
0020:  92 92 04 9E 00 35 00 26 98 31 F2 1D 01 00 00 01   .....5.&.1......
0030;  00 00 00 00 00 00 03 77 77 77 04 64 64 6F 73 03   .......www.ddos.
0040:  63 6F 6D 00 00 01 00 01                           com.....
```

图 2-17　第二次 DNS 请求抓包

下面我们就了解一下 Anti-DDoS 系统如何利用 CNAME 机制进行源认证，这种方式也就是我们前面介绍过的重定向方式，如图 2-18 所示。

① Anti-DDoS 系统部署在授权服务器前，统计到达授权服务器的流量。流量达到告警阈值前，Anti-DDoS 系统只对其进行统计，不进行其他处理



② 流量达到告警阈值后，Anti-DDoS 系统启动源认证，对请求报文进行重定向

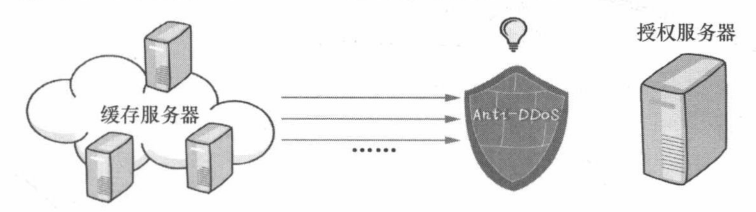


图 2-18　CNAME 防御模式

③ 如果是真实存在的源，Anti-DDoS 系统会正常响应源认证报文

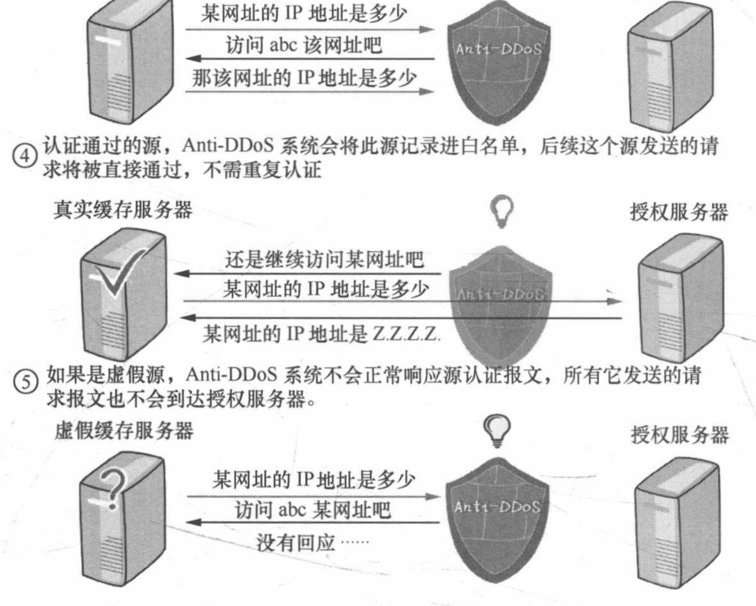


图 2-18 CNAME 防御模式（续）

接下来我们再以一组抓包为例了解此过程。

① 客户端发送 DNS 查询的请求，查询的域名是 www.×××.com，如图 2-19 所示。

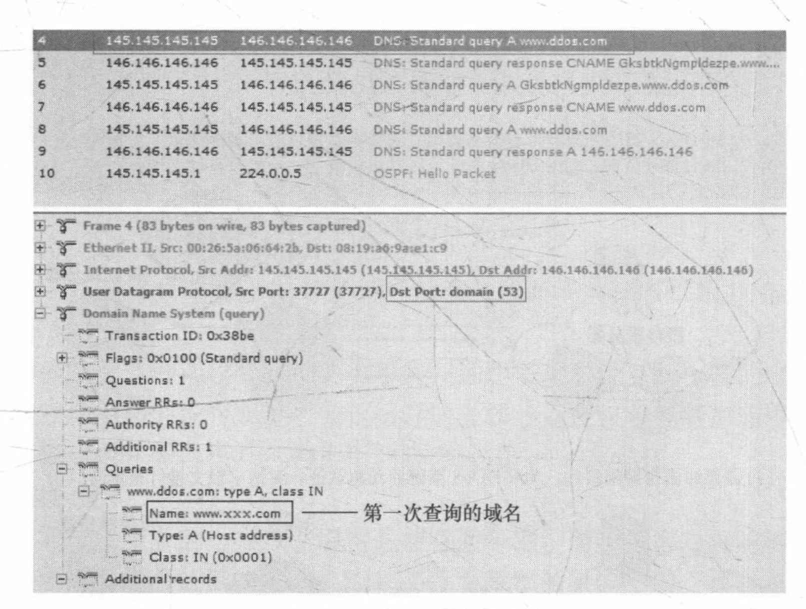


图 2-19 DNS 查询请求抓包

② Anti-DDoS 系统代替 Web 服务器进行回应，并为 www.×××.com 的域名加了一个前缀将其重定向为 GksbtkNgmpldezpe.www.×××.com，让客户端重新请求这个别名，如图 2-20 所示。

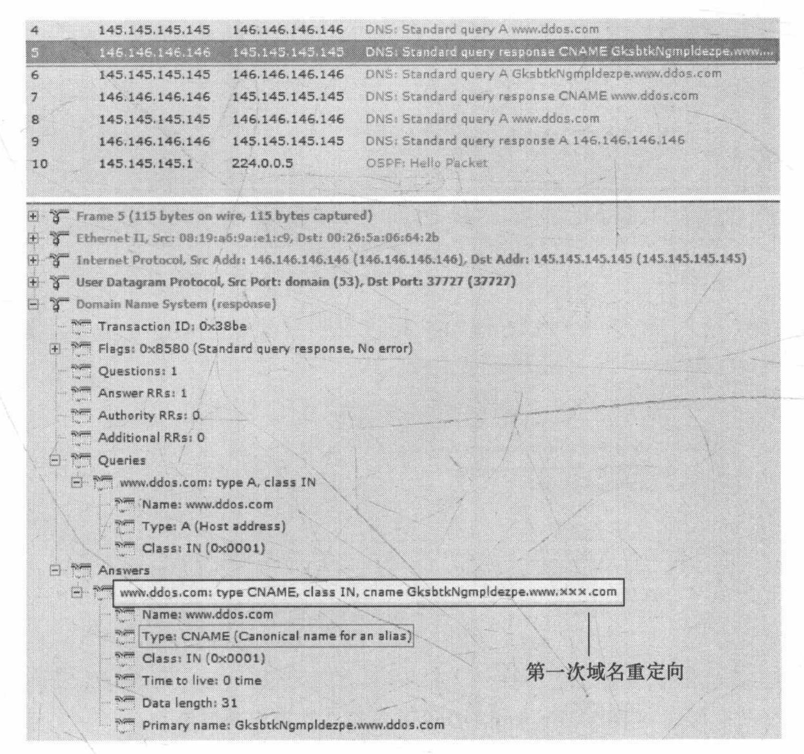


图 2-20 Anti-DDoS 系统代替服务器回应抓包

③ 客户端重新请求重定向后的新域名：GksbtkNgmpldezpe.www.×××.com，如图 2-21 所示。客户端正常响应这个重定向域名后，Anti-DDoS 系统对客户端的源认证就通过了。

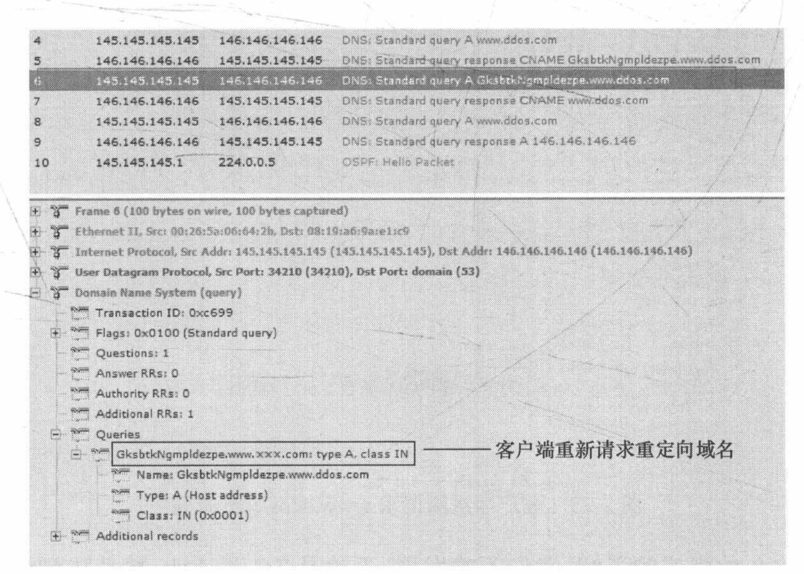


图 2-21 客户端重新请求重定向后的新域名抓包

④ Anti-DDoS 系统第 2 次重定向，如图 2-22 所示，将 GksbtkNgmpldezpe.www.×××.com 再重定向回最初访问的域名 www.×××.com。

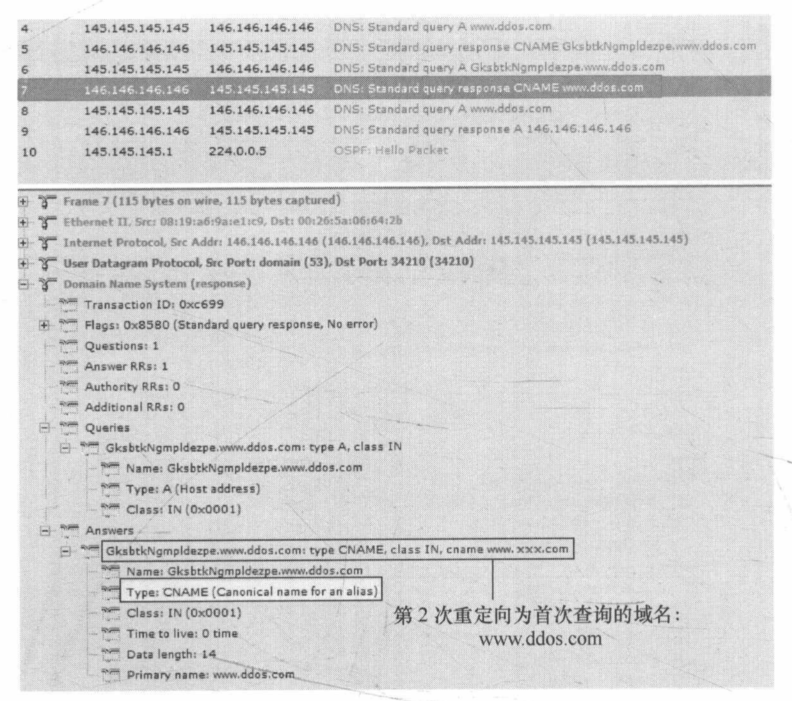


图 2-22 Anti-DDoS 系统第 2 次重定向抓包

⑤ 客户端重新请求 www.×××.com，如图 2-23 所示。这次发送的 DNS 请求报文会直接到达服务器。后续服务器会回应这个域名的解析地址，完成此次 DNS 查询。

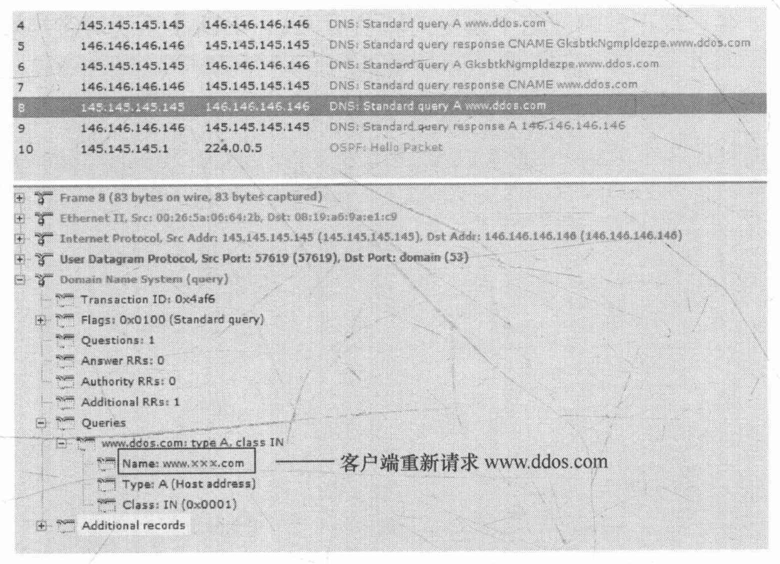


图 2-23 客户端重新请求 www.ddos.com 抓包

通过对这 3 种模式的了解，我们不难发现，无论是 TC 源认证、被动防御还是 CNAME 模式，它们都是利用 DNS 协议对发送请求的客户端是否真实存在所进行的源探测。其中，TC 源认证利用的是 DNS 协议的 TCP 查询方式；被动模式利用的是 DNS 协议的重传机制；而 CNAME 利用的是 DNS 协议的别名机制。

2.4　DNS Reply Flood 攻击与防御

2.4.1　DNS Reply Flood 攻击原理

DNS 查询过程通常都是基于 UDP 的。UDP 是无连接状态的，所以这一弱点很容易被黑客利用。DNS 服务器收到 DNS 回应报文时，不管自己有没有发过解析请求，都会处理这些 DNS 回应报文。DNS reply flood 攻击就是黑客发送大量的 DNS 回应报文到 DNS 缓存服务器，导致缓存服务器因为处理这些 DNS 回应报文而耗尽资源，影响正常业务的过程，如图 2-24 所示。

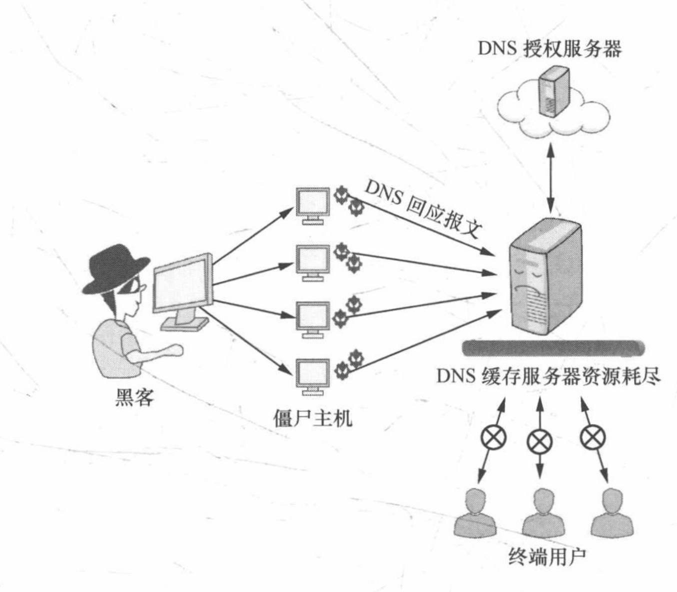


图 2-24　DNS reply flood 攻击原理

DNS reply flood 攻击大多都是虚假源攻击，黑客控制僵尸主机发出的 DNS 回应报文的源 IP 地址通常都是伪造的，是不存在的。所以在防御的时候，系统就可以从回应源 IP 地址的真假性切入，判定这个源 IP 是否是真实源。

2.4.2　华为 Anti-DDoS 系统如何防御 DNS Reply Flood 攻击

针对这种攻击行为，Anti-DDoS 系统一般可使用源认证方式进行防御。源认证的方法就是通过构造一个 DNS 请求报文，试探客户端是否能正常回应的过程，如图 2-25 所示。

源认证过程如下。

① Anti-DDoS 系统部署在受保护服务器前，并统计到达服务器的 DNS 回应报文。当到达服务器的 DNS 回应报文超过告警阈值时，Anti-DDoS 系统启动防御。

② Anti-DDoS 系统收到某个源 IP 地址发来的 DNS 回应报文后，会重新构造一个新

的 DNS 请求报文，然后记录构造查询报文的 Query ID 和源端口号。

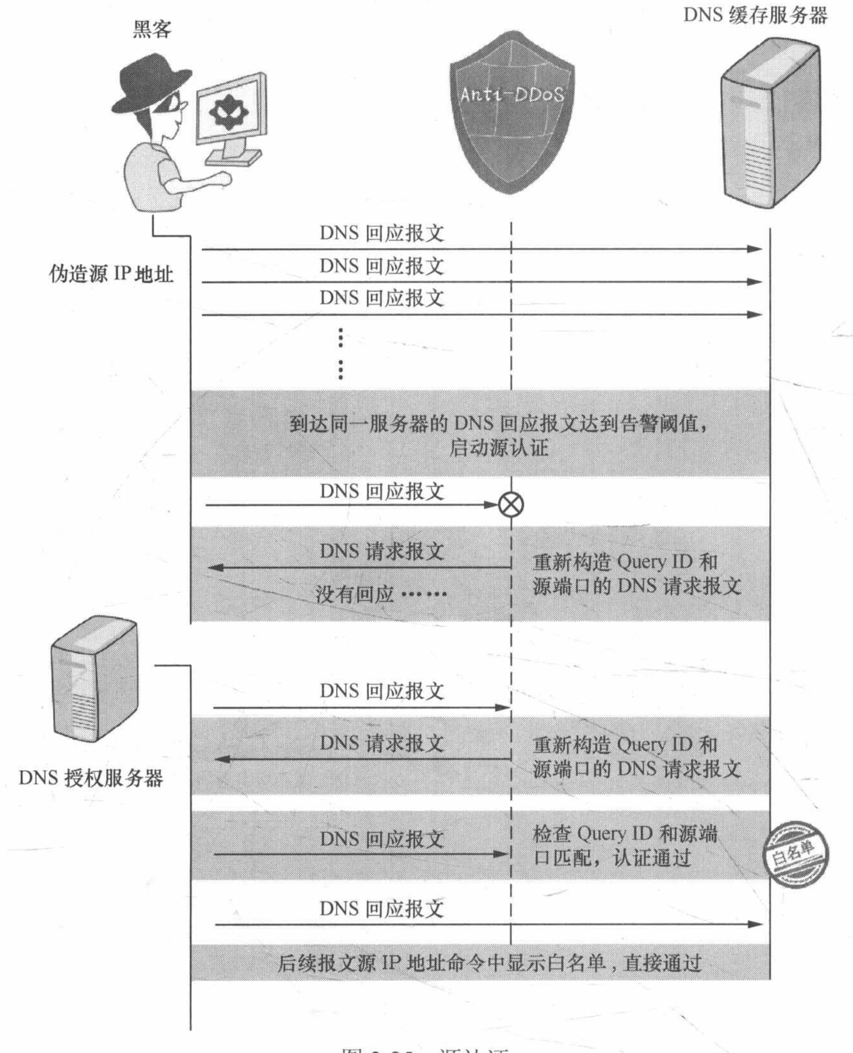


图 2-25　源认证

③ 如果是虚假源，则 Anti-DDoS 系统不会回应这个 DNS 回应报文，认证不通过。

④ 如果是真实 DNS 授权服务器，则 Anti-DDoS 系统会重新回应 DNS 回应报文。

⑤ Anti-DDoS 系统收到 DNS 回应报文后，会将其与之前记录的 Query ID 和源端口号进行匹配。如果完全一致，则系统判定此 DNS 回应报文就是反弹 DNS 请求报文的回应，源认证成功，将其加入白名单。

⑥ 后续这个源再发送的 DNS 回应报文都会被直接通过，直到白名单老化。

这是一种传统的 DNS reply flood 攻击和防御形式。近几年，还有一种升级版的 DNS reply flood 攻击，因为危害性较大，而备受安全界的关注，这就是 DNS 反射攻击。

2.4.3 DNS 反射攻击

DNS 反射攻击是 DNS reply flood 攻击的一种变异，是一种更高级的 DNS reply flood

攻击。

如图 2-26 所示，DNS 服务器是互联网的基础设施之一，网络中有很多开放的免费 DNS 服务器。DNS 反射攻击正是黑客通过这些开放的 DNS 服务器制造的攻击。这种 DNS 反射攻击通常比普通的 DNS reply flood 攻击的攻击性更强，追踪溯源更难。

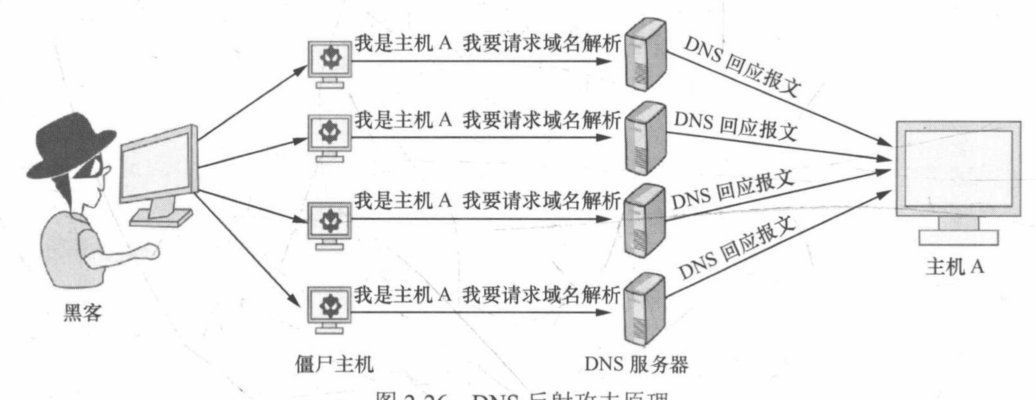


图 2-26 DNS 反射攻击原理

从图 2-26 中我们可以看到，黑客将自己的源 IP 地址伪造成被攻击目标（主机 A）的 IP 地址，然后向网络中开放的 DNS 服务器发送大量的查询请求。黑客通过伪造 DNS 请求报文的源 IP 地址，控制 DNS 回应报文的流向，这些 DNS 回应报文都会被引导到被攻击目标，导致被攻击目标的网络拥塞，从而拒绝正常服务。而全球有几千万台开放式的 DNS 服务器，这些服务器的接入带宽往往都比较高，而且，DNS 回应报文的大小通常也是 DNS 请求报文的几倍甚至几十倍，因此，这种攻击还可达到放大攻击的效果。对于控制成千上万台僵尸主机的黑客来说，制造几 GB 乃至数十 GB 的 DNS 攻击流量并不太困难。

DNS 反射攻击和前面介绍的传统 DNS reply flood 攻击有两点本质的不同。

① 传统 DNS reply flood 攻击的攻击目标一般是 DNS 缓存服务器；而 DNS 反射攻击的攻击目标一般是客户端。

② 传统 DNS reply flood 攻击大多是虚假源攻击，而在 DNS 反射攻击中，DNS 请求报文都是真实的，DNS 回应报文也都是真实的，这是由网络中真实的 DNS 服务器发出的，属于真实源攻击。在这种情况下，源认证方式便不适用 DNS 反射攻击了。

Anti-DDoS 系统借鉴防火墙的会话表机制，利用 DNS 交互过程中 DNS 请求报文首包创建会话的机制，防御 DNS 反射的放大攻击，如图 2-27 所示。

Anti-DDoS 系统对 DNS 反射攻击采用的防御手段就是会话检查。会话表五元组信息包含：源 IP 地址、目的 IP 地址、源端口、目的端口和协议。当 DNS 请求报文经过 Anti-DDoS 系统时，Anti-DDoS 系统会创建一张会话表，记录 DNS 请求报文的这五元组信息。当 Anti-DDoS 系统再收到 DNS 回应报文时，就会查会话表：如果它与会话表匹配，系统就判定它是真实的回应报文，允许它通过；如果它与会话表匹配，则系统判定这个回应报文为攻击报文，禁止它通过。

除了源认证和会话检查以外，DNS 攻击还可以通过限速的方式被防御。DNS 限速有两种：域名限速和源 IP 地址限速，针对 DNS 请求报文和 DNS 回应报文都生效。

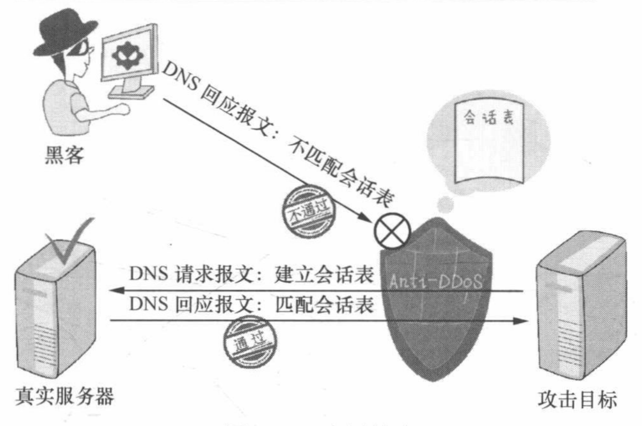


图 2-27 会话检查

（1）域名限速

如果某个域名的 DNS 请求或回应报文速率过高，我们可以针对这个域名进行限速。

通常某个域名遭受的访问量一直高，但突然有一天某访问量增长到平时的很多倍，此时我们可判断这个域名可能遭受了攻击。域名限速就是指在资源有限的情况下，每天只有一定数量的资源被提供，先到先得。

域名限速可以有针对性地限制某个特定域名，而不影响其他域名的正常请求。

（2）源 IP 地址限速

源 IP 地址限速和域名限速相比属于另一个维度的限制。如果某个源 IP 地址域名解析的速率过大，源 IP 地址限速就可以有针对性地限速这个源 IP 地址的 DNS 请求报文或者 DNS 回应报文，这样也不会对其他源造成影响。

现在，这种利用网络基础架构发动的攻击越来越多，比如 2.1 节介绍的“龙卷风”、2.4 节介绍的 DNS 反射攻击，还有后续我们将要介绍的 DNS 缓存投毒攻击、HTTP 攻击等。作为互联网的基础设施，DNS 服务器和其他各种服务器的安全稳定运行是至关重要的，也是网络工程师在部署网络设备时需要重点考虑的问题。

2.5 DNS 缓存投毒攻击与防御

2.5.1 事件回顾

根据 Google 的 DNS 服务商 OpenDNS 所述，曾有一名黑客通过将 Google 的域名服务器（ns1.google.com、ns2.google.com）修改成 CloudFlare 的 IP（173.245.59.108, 173.245.58.166）来重定向访客。网民在访问 Google 主页的时候，看到的不是 Google 的搜索页面，而是一张自拍照。

这些事件其实是黑客篡改了域名和 IP 地址的映射关系，将用户访问的域名指向了其

他 IP 地址所导致的。DNS 篡改可能发生在各个环节，比如在客户端侧、在授权服务器端，或者在缓存服务器端。下面我们就来看看比较常见的几种篡改方式。

2.5.2 路由器 DNS 劫持

黑客利用路由器的漏洞入侵受害者的路由器，篡改路由器中 DNS 服务器的地址，将该 DNS 服务器地址指向恶意的 DNS 服务器地址。这种篡改对于用户来说是最可怕的，一旦发生了这种情况，那么这个用户访问的每一个域名，都可能会被解析成其他恶意地址。

TP-Link 路由器的劫持事件，就是黑客构造了一个恶意 Web 页面（页面的功能是自动登录路由器并修改 DNS 地址），然后，再构造一个 URL 发送给受害者，当受害者点击这个链接的时候就访问了恶意页面。攻击要想成功的前提是黑客必须知道 TP-link 路由器的登录账号和密码。然而实际上，大多数人都会使用 TP-link 路由器厂商预置的默认密码，这就给了黑客实施攻击的机会，导致路由器的 DNS 服务器的 IP 地址很容易被篡改为恶意的 IP 地址。

这种劫持方式不容易被发现，受害者只要输入真实域名或者合法网站地址，黑客就可将其重定向到一个恶意网站上。一旦这种情况发生，对于受害者来说后果是非常可怕的。受害者访问的每一个域名可能都是假的。他看到的淘宝页面可能不再是淘宝页面，登录的网银可能也不再是网银，用户的各种敏感信息都会受到严重威胁，如图 2-28 所示。



图 2-28 路由器 DNS 劫持

对于这种方式，最有效的防御办法就是用户为路由器设置安全系数高的密码，然后定期修改密码。另外，对于不明链接，我们也建议用户不要随便点击。

2.5.3 授权服务器的修改

直接在授权服务器上修改域名和 IP 地址的映射关系是最直接的一种方式。黑客如果使用这种方式作为攻击的手段，需要通过特殊手段获取授权服务器的管理员权限，此方式的难度系数其实是非常大的。

当然，也有另一种可能，就是出于某种特殊目的，管理员直接修改授权服务器上的域名和 IP 地址的映射关系，这种类型比较少见，也不是我们能控制的，这里我们不进行详细介绍。

2.5.4 缓存服务器的修改

缓存服务器的修改就是常见的 DNS 缓存投毒，是一种典型的 DNS 攻击，下面我们一起来了解一下黑客如何篡改缓存服务器。

前文也提到过：缓存服务器并不知道域名和 IP 地址的映射关系，一旦缓存服务器从

授权服务器获取了映射关系后，会将其在内存中存储一段时间，直到记录老化。老化时间由 DNS 回应报文中的 TTL 决定。在这个有效期内如果再有客户端请求这个相同域名的解析，缓存服务器就会直接用缓存中的 IP 地址进行回应。记录老化以后，如果有客户端再次请求这个域名时，缓存服务器就会重新向授权服务器请求这个域名的解析。

如图 2-29 所示，缓存投毒攻击就是黑客伪造了恶意的 DNS 回应报文，导致缓存服务器无意中将恶意的域名和 IP 地址映射关系存储到自己的缓存中。当客户端再通过缓存服务器请求这个域名解析时，就会被指向恶意主机。

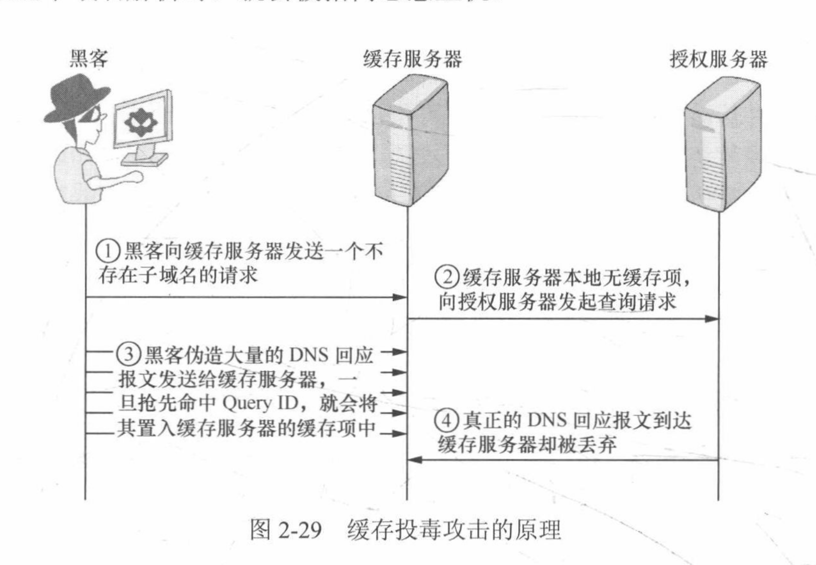


图 2-29 缓存投毒攻击的原理

缓存投毒攻击过程如下。

① 黑客向 DNS 缓存服务器发送一个不存在的子域名，请求解析。

② 缓存服务器查找本地缓存项查不到该域名，就会向授权服务器发起查询请求。

③ 在授权服务器回应这个请求前，黑客就会伪造大量的 DNS 回应报文发向缓存服务器。

为了达到攻击的目的，黑客伪造的 DNS 回应报文的源 IP 地址必须是授权服务器的源 IP 地址，目的端口也必须是缓存服务器的源端口；同时，DNS 回应报文的 Query ID 和 DNS 请求报文的 Query ID 也要一致。

源 IP 地址和目的端口都很好伪造，但是成功伪造 Query ID 是有一定难度的。因此黑客伪造大量 DNS 回应报文时，会不断变换 Query ID 字段，可能就会有一个 Query ID 字段命中 DNS 请求报文的 Query ID。一旦该 Query ID 先于授权服务器被发送给缓存服务器，缓存服务器就会将黑客发送的伪解析 IP 地址作为解析地址，保存到本地的缓存表中。

④ 之后，当授权服务器再将真正的回应报文发送到缓存服务器时，缓存服务器也不会接收，直接将其丢弃。

在 DNS 缓存服务器中，如果仅仅伪造的子域名的解析地址是假的其实也没有多大影响。毕竟黑客利用投毒的这个子域名通常都是不存在的，正常客户端也不会请求这个不存在的子域名。

但是我们再仔细了解一下图 2-30 所示的 DNS reply 报文就会发现：第一个框内是对该子域名的解析地址；第二个框内则是主域名 ddos.com 所在的 DNS 授权服务器和 IP 地址的对应关系，授权服务器在回答缓存服务器请求时，也会将这部分内容一起发送过去，缓存服务器不仅仅会存储子域名的解析地址，还会将主域名的解析地址一并更新到自己的缓存列表中。这样后续再有客户端请求这个主域名时，也会一并被指向虚假的 IP 地址。

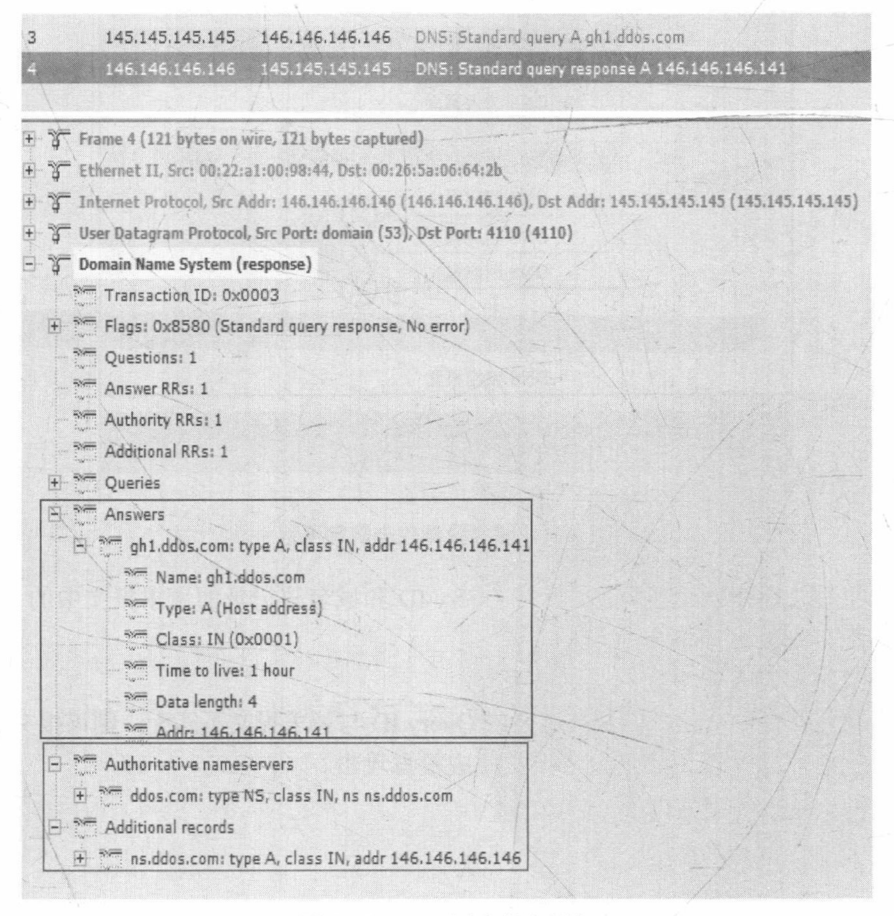


图 2-30 DNS 回应报文抓包

对于缓存投毒攻击，Anti-DDoS 系统采用会话检查模式进行防御。如图 2-31 所示，在防御过程中，Anti-DDoS 系统检查 DNS 回应报文的会话五元组信息（源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议），Query ID 和域名是否与缓存服务器发出的 DNS 请求报文一致。

缓存投毒攻击防御流程如下。

① 当缓存服务器向授权服务器发出域名查询请求时，Anti-DDoS 系统记录会话信息及请求报文中的 Query ID 和域名。

② Anti-DDoS 系统收到回应报文后，需检查会话五元组、回应报文中的 Query ID 和域名与请求报文中的 Query ID 和域名是否匹配。

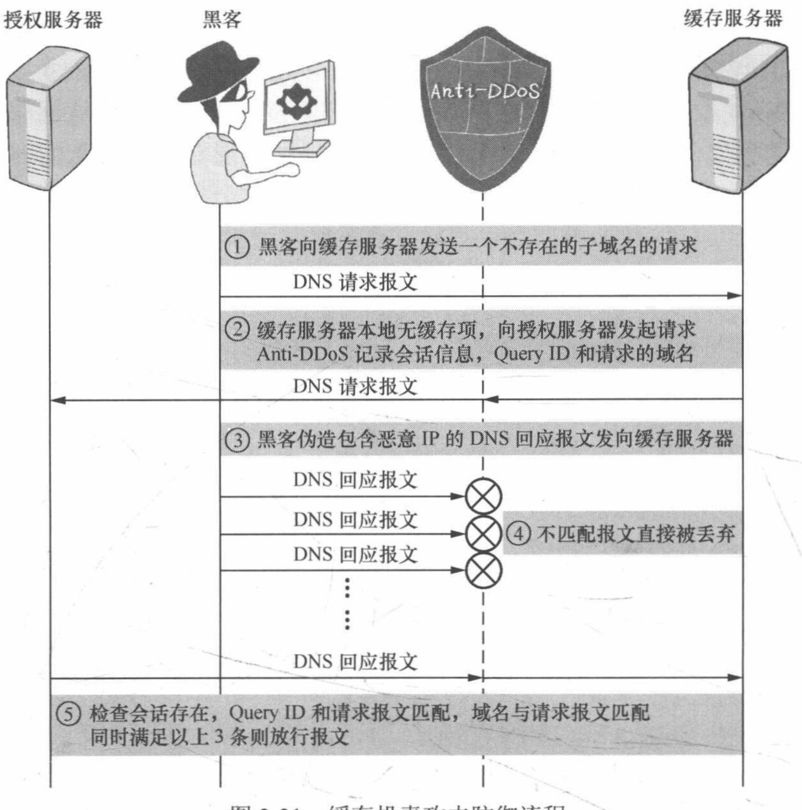
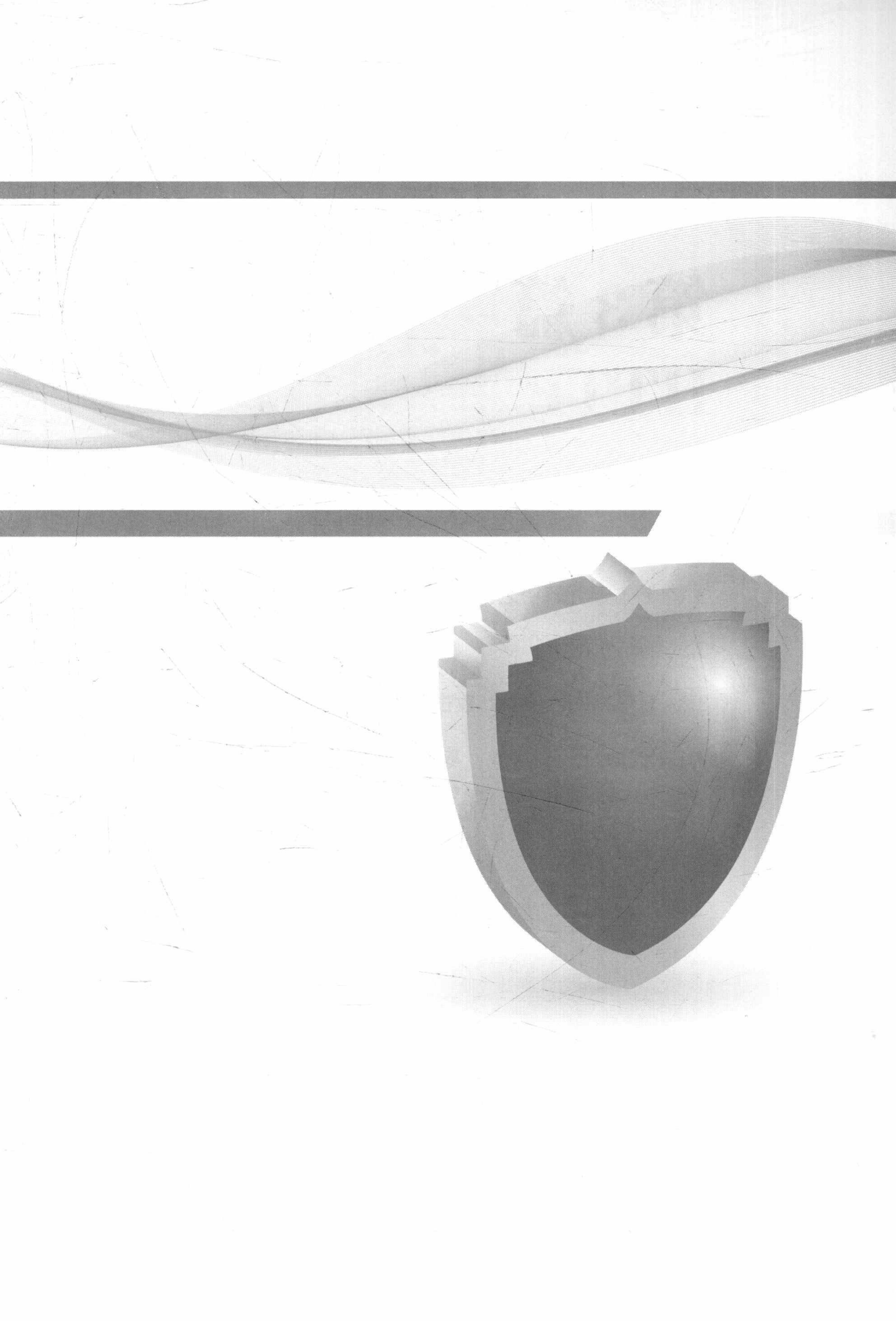


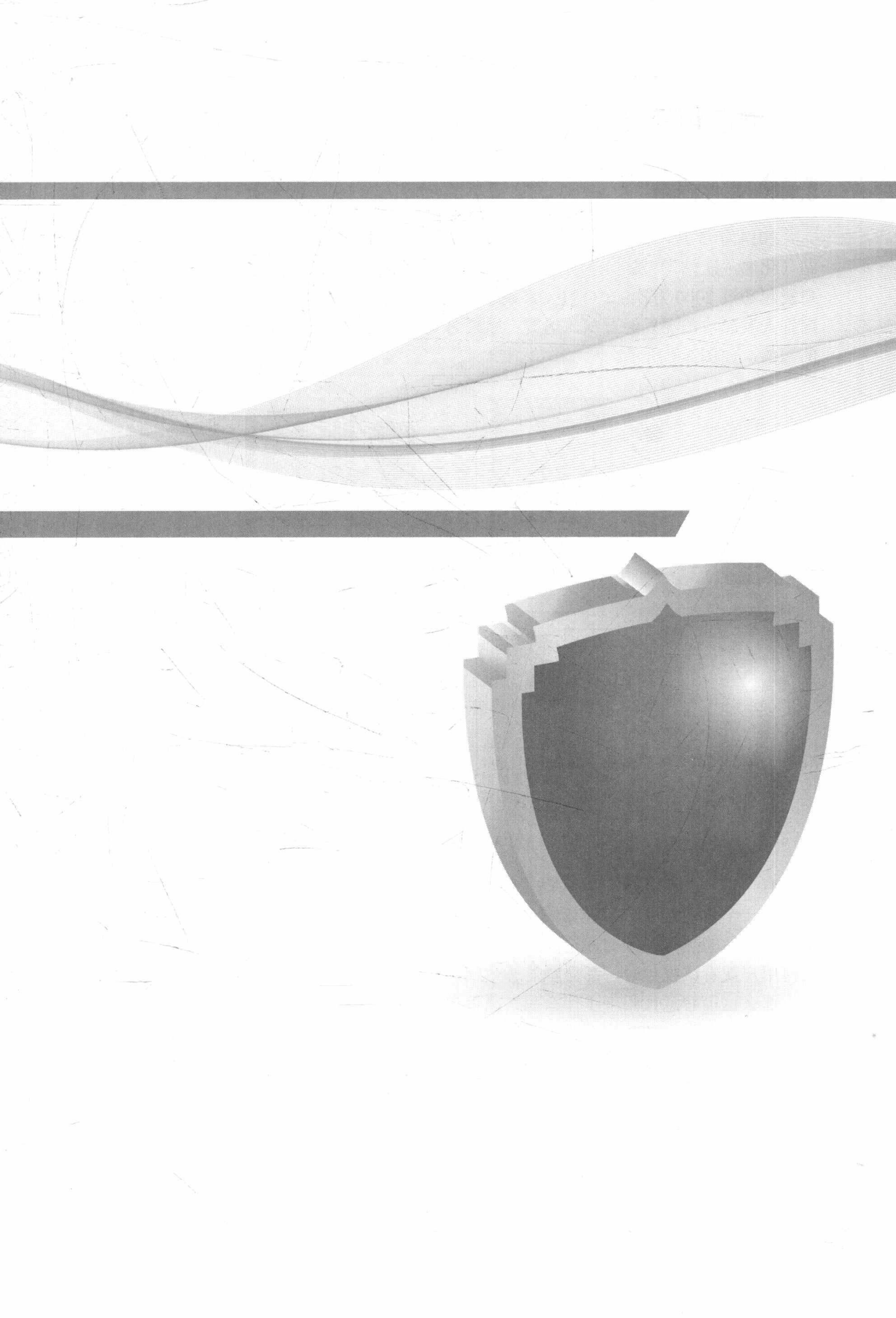
图 2-31　缓存投毒攻击防御流程

- 如果报文命中会话五元组，并且 Query ID 和域名与记录的请求报文中的 Query ID 和域名匹配，则放行该报文。
- 如果报文没有命中会话，则被丢弃。

如果该报文命中会话，但是其域名或 Query ID 与请求报文不匹配，则该报文被丢弃，同时该会话被删除，以免后续投毒报文完成投毒攻击。



第3篇 HTTP



3.1 热点事件解密之：跨站脚本攻击事件

3.1.1 事件回顾

2014 年 5 月，日本某 CDN 服务商声称，自己的一位客户的服务器遭遇了某视频网站（化名“H 站”）发起的 DDoS 攻击，期间总共有超过 2 万的网民通过 H 站向这位客户发起超过 2000 万次的 HTTP Get 请求。如此知名的视频网站，怎么会甘冒不韪，公然向别人发起攻击呢？经过深入追究，原来 H 站是在未知的情况下被黑客利用，成为攻击的源头，如图 3-1 所示。

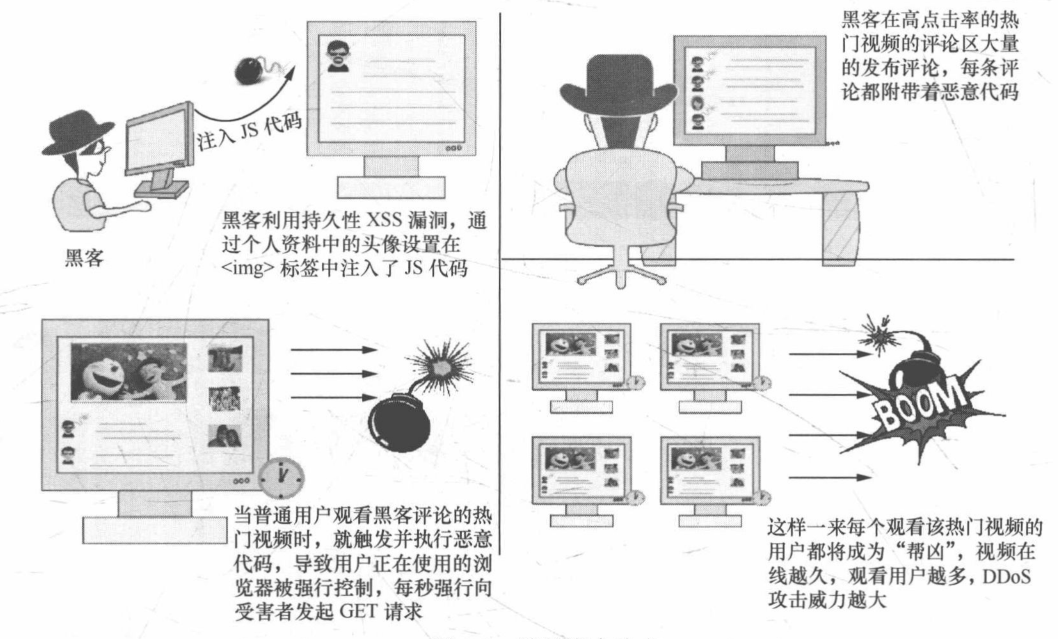


图 3-1 跨站脚本攻击

有句话叫“趁虚而入”，H 站上恰好就有这么一个漏洞给了黑客“打劫”的机会。黑客注册一个该网站账户，在该账户的头像中注入恶意代码（JavaScript），然后用这个账户在该网站的热门视频的评论区发布大量的评论。这样，每条评论都附带着恶意代码。任何用户观看该视频时，都会触发恶意代码，因而控制 H 站中某一用户的浏览器。

那么这段恶意代码干了什么呢？简单说，这段代码就是在用户不知情的情况下，定时向受害者发起 HTTP 访问请求。这个定时器设定的时间为每秒发起一次请求。

也就是说，某用户观看 H 站视频时，他的浏览器会每秒向受害者发起一次请求。如果该用户观看 30 分钟的视频，他就会向受害者发起 1800 次请求。H 站这样的大型视频网站，同时在线观看热门视频的用户都是成千上万级别的，黑客在多个热门视频下发布海量评论，轻松获得无数“肉鸡”。攻击效果可想而知了。

下面我们就分析一下这次攻击事件。在分析之前，我们先简单回忆下 HTTP 的基础。

3.1.2　HTTP 基本知识

HTTP（HyperText Transfer Protocol，超文本传输协议），它最基本的交互流程如图 3-2 所示。

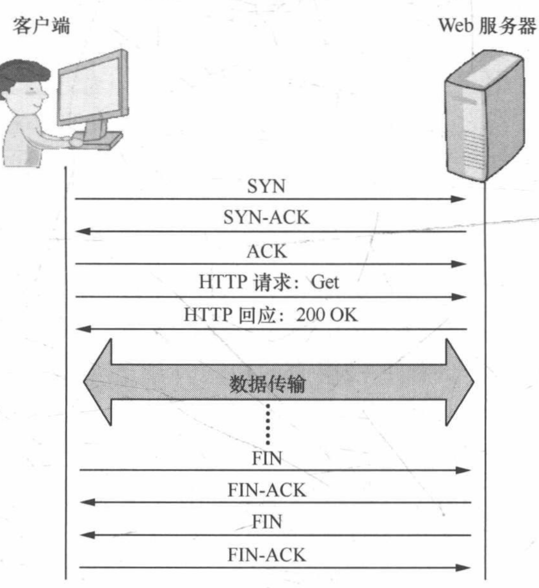


图 3-2　HTTP 报文交互过程

完成 TCP 三次握手后，客户端向服务器发起 HTTP 请求。正常情况下，服务器回应 200 OK，在应答中添加应答长度，然后开始传输数据。

HTTP 还有一种重定向的交互流程，如图 3-3 所示。

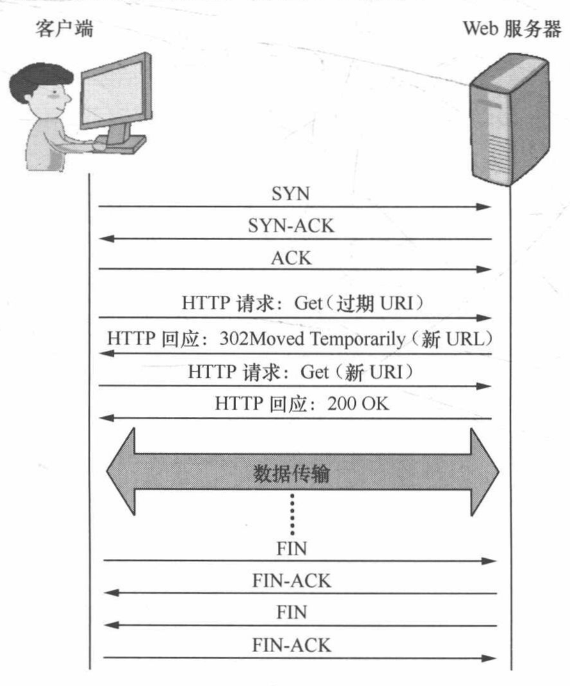


图 3-3　HTTP 重定向交互过程

完成 TCP 三次握手后，客户端向服务器发起 HTTP 请求。如果客户端请求的这个 URL 是过期的，服务器就会回应客户端 302 重定向报文，并携带新的 URL 地址。客户端再重新向新的 URL 地址发起请求，服务器回应 200 OK，并开始传输数据。

3.1.3 华为 Anti-DDoS 系统的解决方案

HTTP 是一种基于 TCP 的应用层协议。HTTP 类的攻击，它最高效的防御方式就是源认证方式进行校验。华为 Anti-DDoS 解决方案可以感知 TCP 和 HTTP，其也可以针对攻击源进行多层级的源认证和校验。

源认证体系主要有以下 3 个层面。

（1）TCP/IP 源认证

TCP/IP 源认证一般用于 TCP 三次握手还没建立成功前，验证攻击源的 TCP/IP 是否真实可信，比如 IP 源认证是对 IP 层面的校验，认证这个源是不是真实存在的；TCP 代理和首包丢弃校验是对于 TCP 栈层面的校验，用于判断是否是这个源发出的真实请求。

很显然上述攻击事件已经完成了 TCP 三次握手，不属于 TCP/IP 范畴，关于 TCP/IP 源认证的防御机制，我们会在后面详细介绍，本节着重介绍应用层源认证。

（2）应用层源认证

如果“肉鸡”使用工具调用真实的 TCP/IP 发动攻击，则 TCP/IP 源认证无法识别是否是攻击。我们必须启用应用层源认证，比如利用 HTTP 302 重定向请求，认证客户“浏览器”是否可信，如图 3-4 所示。

（3）用户源认证

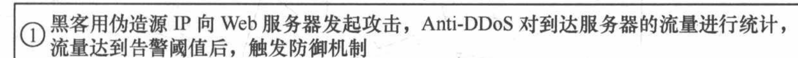
客户端是真实的基础上，进一步验证是否由真实用户发出的请求，而不是僵尸浏览器被黑客控制强制发出的请求。针对这种情况，终极的手段就是，人机交互，输入验证码和图片运算。验证码机制就是对登录用户的一次安全验证，判断一下是不是真实用户发起的请求。如果是 DDoS 工具发起的请求，则无法自动响应验证请求，如图 3-5 所示。

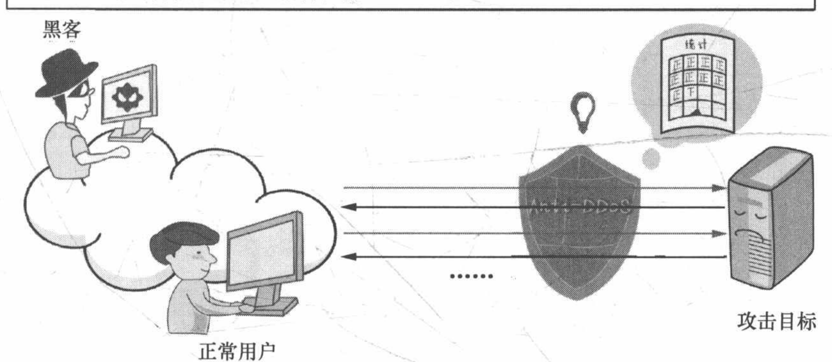
我们再回到前面的攻击事件上来。攻击报文是由浏览器发出的请求，没有人为参与，源 IP 是真实存在的，浏览器也是真实存在的，但是请求行为是虚假的。在防御 Anti-DDoS 时，它就要识别出 HTTP 请求中，哪些是真实的用户发送的请求，哪些是僵尸浏览器发的请求。浏览器具有完整的 HTTP 校验机制，对于 302 重定向报文，浏览器可以自行完成交互过程，无须用户参与。因此，302 重定向方式识别不了僵尸浏览器，只有通过验证码这种需要人机交互的方式来识别攻击报文。

对于 HTTP 攻击防御，第二层提到的 302 重定向和第三层的验证码方式都是非常有效的针对虚假源攻击的防御手段。只要客户端具备完善的 302 重定向机制，就可以通过 302 重定向源探测方式识别虚假源。

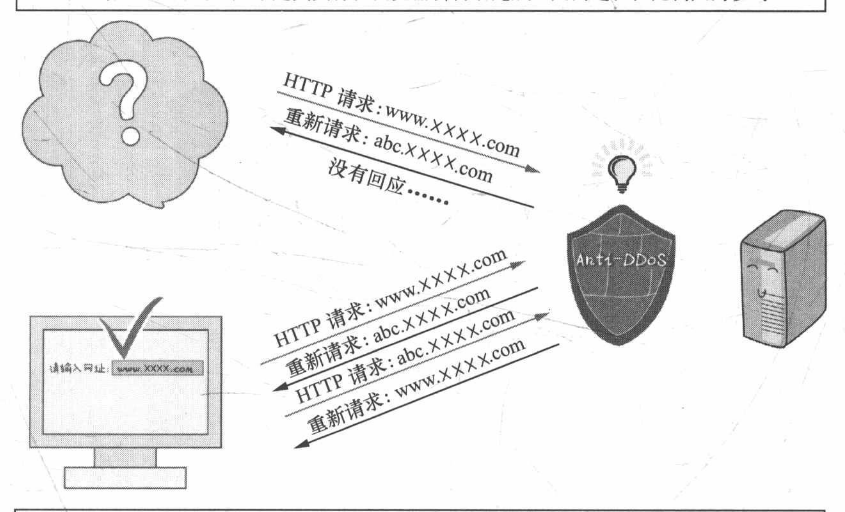
还有一种特殊情况，网络中有 HTTP 代理服务器时，只要有一次源认证通过，Anti-DDoS 就会将代理服务器 IP 地址加入白名单。黑客如果利用代理服务器 IP 绕过源认证，就会导致防御失败。这种情况下，源认证功能就要配合代理检查功能一起使用，检测 HTTP 请求是否为通过代理发出的。如果是，Anti-DDoS 会从 HTTP 报文中获取请

求者的实际 IP 地址，并将通过认证的真实 IP 地址和代理服务器 IP 地址加入白名单，后续只有此实际源 IP 地址发送的报文才能直接通过，其他源 IP 发送报文时，Anti-DDoS 会对其进行源认证，达到防御效果。


①黑客用伪造源 IP 向 Web 服务器发起攻击，Anti-DDoS 对到达服务器的流量进行统计，流量达到告警阈值后，触发防御机制



②启动防御后，Anti-DDoS 拦截 HTTP 请求报文，并反弹重定向到客户端，如果是虚假源，则不会响应重定向。如果是真实源，浏览器会自动完成重定向过程，无需人为参与



③Anti-DDoS 将正常响应重定向的客户端加入白名单，后续此客户端发送的 HTTP 请求可直接通过，送到 Web 服务器

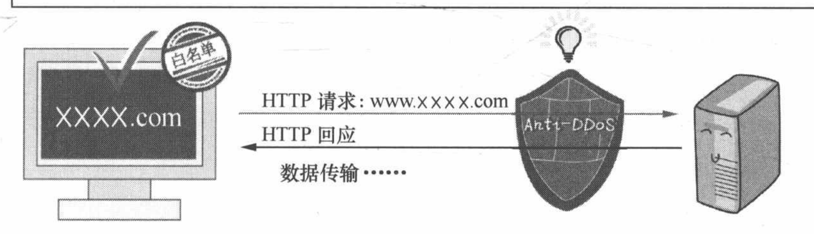


图 3-4 HTTP 源认证

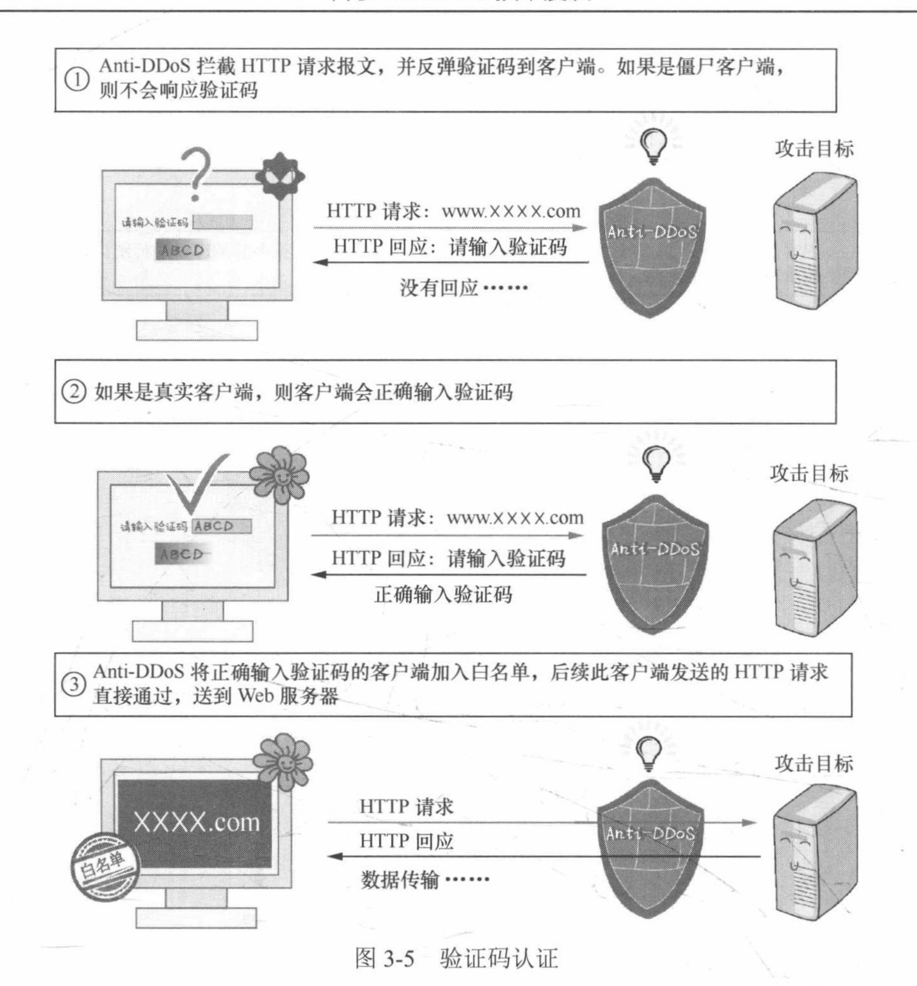


图 3-5 验证码认证

3.2 HTTP 解析

大家可能在想，上网看视频居然会触发 DDoS 攻击，而每一个观看视频的人在不知不觉中就变成了黑客的帮凶。我们只有了解攻击才能更好地防御。

3.1 节讲述的事件中，黑客利用视频网站的 XSS 漏洞（Cross Site Scripting，跨站脚本攻击），“劫持”观看视频者的流量，并向受害者发起海量的 HTTP 请求。最终，数以千万计的 HTTP 请求形成了一次规模巨大的 DDoS 攻击，使受害者无法正常上网。

攻击源头和攻击方式都与 HTTP 有关。HTTP 是当前使用最广泛的协议，我们浏览网页、看新闻、查资料都是 HTTP 在背后默默地工作。

3.2.1 HTTP 请求报文

HTTP 是一种请求/响应式的协议，客户端向服务器发起请求，服务器收到请求后，向客户端返回响应信息。HTTP 报文分为请求报文和响应报文，HTTP 请求报文的格式如图 3-6 所示。

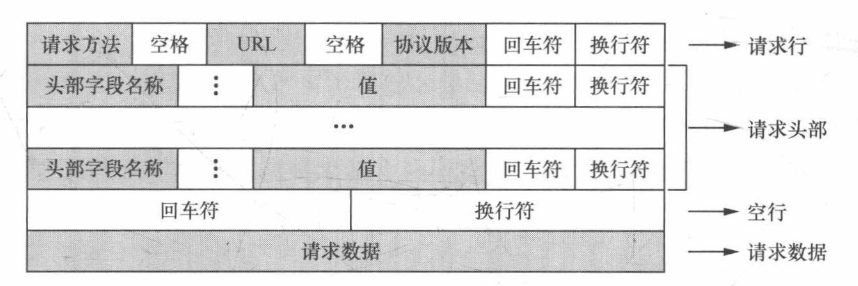


图 3-6 HTTP 请求报文格式

我们结合 HTTP 请求报文的抓包信息来学习各个字段的含义，如图 3-7 所示。

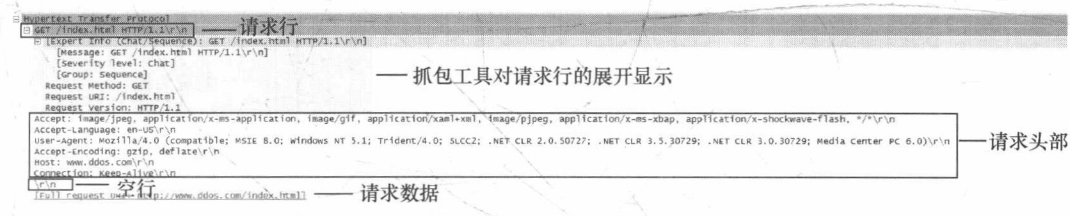


图 3-7 HTTP 请求报文抓包

HTTP 请求报文由请求行、请求头部、空行和请求数据 4 个部分组成，各部分的具体解释如下。

（1）请求行

请求行由请求方法字段、URL 字段和协议版本字段组成，这 3 个字段之间使用空格分隔，最后由回车符\r+换行符\n 结束。例如，GET /index.html HTTP/1.1\r\n。这里顺便提一下 URL 和 URI，URL 全称是（Uniform Resource Locator，统一资源定位），URI 全称是（Uniform Resource Indentifier，统一资源标识）。一般情况下我们看到浏览器处理的是 URL，而在 HTTP 规范中会使用 URI。

请求行中值得关注的是请求方法字段，常用的请求方法有 GET，它表示客户端从服务器获取数据，即要求服务器将 URL 定位的资源放在响应报文中，返回给客户端；POST 表示客户端向服务器提交数据，由服务器进行处理，如表单提交、账号登录等操作使用的就是 POST 请求方法。

GET 和 POST，这两种请求方法经常会被用来进行 DDoS 攻击，例如在 H 站攻击事件中，广大“帮凶”使用的就是 GET 请求方法，它能向受害者发起海量的 HTTP 请求。除了这两种请求方法外，HTTP 还支持 HEAD、PUT、OPTIONS、DELETE 等请求方法，此处不再赘述。

（2）请求头部

请求头部由“关键字/值”对组成，每行一对，关键字和值之间使用英文“:”分隔，最后由回车符+换行符结束。请求头部中可以包含多个类型的关键字，这些关键字用于通知服务器有关于客户端请求的信息。

（3）空行

空行里面包括回车符和换行符，它表示请求头部结束，接下来为请求数据部分。这一行必不可少，它用来告知服务器以后不再有请求头，如果服务器没有收到这个空行则

会一直保持连接。

（4）请求数据

请求数据是 HTTP 报文的载荷，即 HTTP 报文要传输的内容。请求数据部分是可选的，请求方法是 GET 时，HTTP 报文中就不包含请求数据；请求方法是 POST 时，HTTP 报文中包含请求数据。

3.2.2 HTTP 响应报文

了解 HTTP 请求报文的格式后，我们看一看 HTTP 响应报文的格式，如图 3-8 所示。

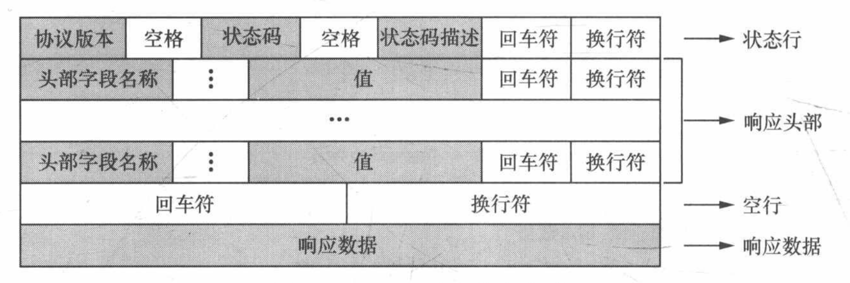


图 3-8 HTTP 响应报文格式

我们结合 HTTP 响应报文的抓包信息来学习各个字段的含义，如图 3-9 所示。

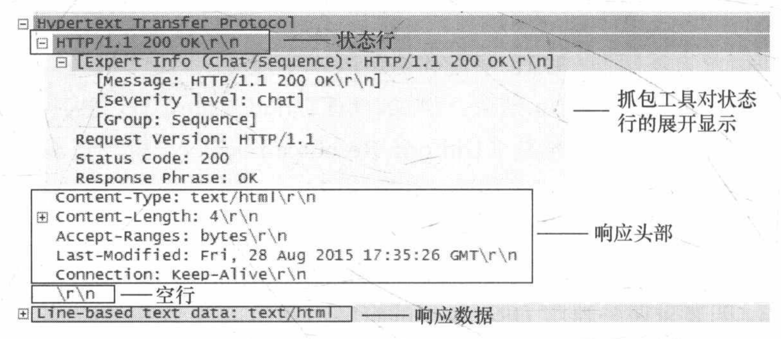


图 3-9 HTTP 响应报文抓包

HTTP 响应报文由状态行、响应头部、空行和响应数据 4 个部分组成，各部分的具体解释如下。

（1）状态行

状态行由协议版本字段、状态码字段和状态码描述字段组成，这 3 个字段之间使用空格分隔，最后由回车符+换行符结束。例如，HTTP/1.1 200 OK\r\n。

状态行中值得关注的是状态码字段，常用的状态码有 200、302、307、404、408。200 表示服务器响应成功；302 表示请求方法为 GET 时，服务器告知客户端需要重定向到新的 URL；307 表示请求方法为 POST 时，服务器告知客户端需要重定向到新的 URL；404 表示服务器无法找到所请求 URL 对应的资源；408 表示请求超时，客户端需要重新提交请求。

（2）响应头部

响应头部与请求头部类似，也是由“关键字/值”对组成，每行一对，关键字和值之

间使用英文“:”分隔，最后由回车符+换行符结束。响应头部中可以包含多个类型的关键字，这些关键字用来通知客户端有关于服务器响应的信息。

（3）空行

响应头部的后面也会有一个空行，它里面包括回车符和换行符，表示响应头部结束，接下来为响应数据部分。

（4）响应数据

响应数据是服务器返回给客户端的信息，图 3-9 中显示的响应数据是一个 HTML 网页，其也可以是图片、视频等信息。

上文我们介绍了 HTTP 报文的格式，并对其中的关键字段进行了解释，下面我们再来了解一下 HTTP 的基本交互流程。我们提到过，HTTP 是一种请求/响应式的协议，客户端与服务器建立 TCP 三次握手后，客户端向服务器发出 HTTP 请求，服务器向客户端返回 HTTP 响应，在一来一回之间完成了数据的传输，如图 3-10 所示。

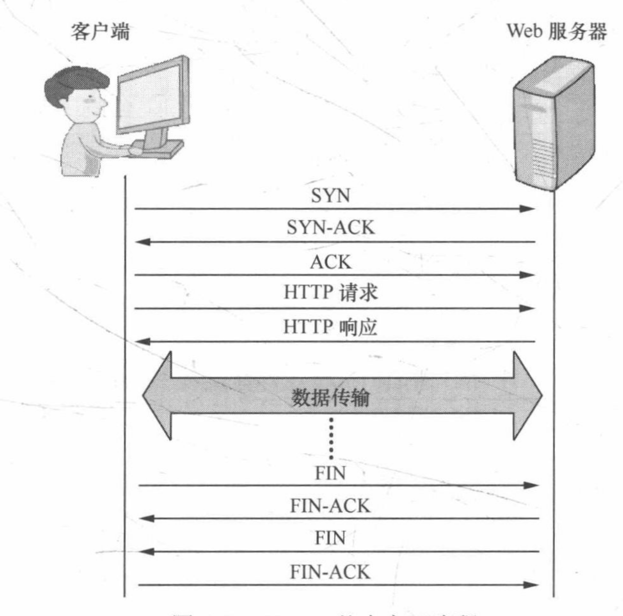


图 3-10　HTTP 基本交互流程

学习完前面的内容，相信大家对 HTTP 有了更进一步的认识。目前 Internet 上运行着多种基于 HTTP 的 Web 信息系统，这些 Web 信息系统存在的安全问题必须重视。

回到 DDoS 攻击上来，针对 HTTP 的 DDoS 攻击主要有利用 GET 和 POST 请求方法的 Flood 类攻击、利用 HTTP 实现机制的慢速类攻击。

3.3　HTTP GET Flood 攻击与防御

HTTP GET Flood 攻击的原理很简单，攻击者利用攻击工具或者操纵僵尸主机，向目标服务器发起大量的 HTTP GET 报文，请求服务器上涉及数据库操作的 URI 或其他消耗系统资源的 URI，造成服务器资源耗尽，无法响应正常请求。

华为 Anti-DDoS 系统防御 HTTP GET Flood 攻击的常用手段是源认证，这种防御方式适用于以客户端为浏览器的场景，因为浏览器支持完整的 HTTP，可以正常回应 Anti-DDoS 系统发出的探测报文。源认证最常用的方式是 302 重定向认证。

3.3.1 302 重定向认证

302 重定向认证的原理是 Anti-DDoS 系统代替 Web 服务器向客户端响应 302 状态码（针对 GET 请求方法的重定向），告知客户端需要重定向到新的 URL，以此来验证是否是真实客户端，如图 3-11 所示。真实客户端的浏览器可以自动完成重定向过程，通过认证；虚假源或者一般的攻击工具没有实现完整的 HTTP，不支持自动重定向，无法通过认证。

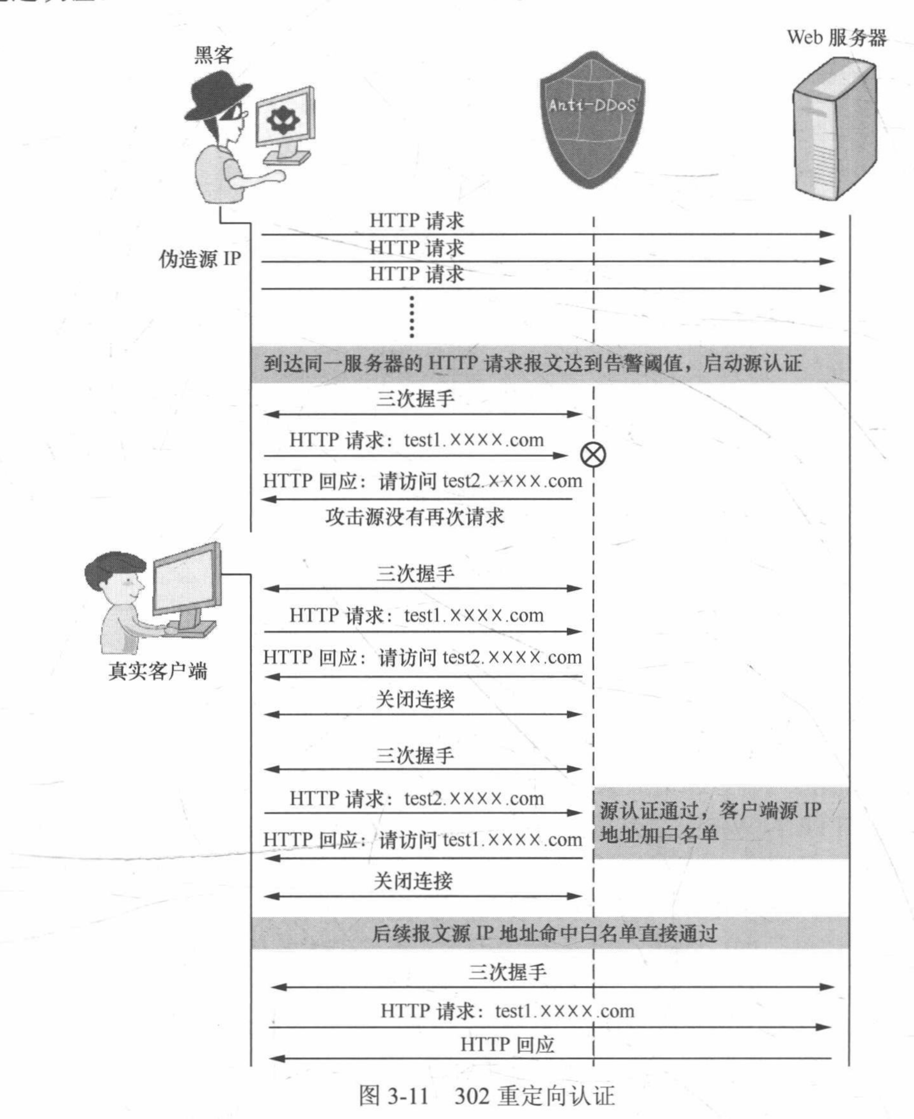


图 3-11 302 重定向认证

当连续一段时间内去往目标 Web 服务器的 HTTP GET 请求报文超过告警阈值后，Anti-DDoS 系统启动源认证机制。源认证机制启动后，Anti-DDoS 系统将会代替 Web

服务器与客户端建立 TCP 三次握手。Anti-DDoS 系统拦截 HTTP 请求，代替 Web 服务器回应 302 状态码，将客户端的访问重定向到一个新的 URI。如果这个源是虚假源，或者不支持完整 HTTP 的攻击工具，不会向新的 URI 发起请求。如果这个源是真实客户端，则会向新的 URI 发起请求。Anti-DDoS 系统收到请求后，将该客户端的源 IP 地址加入白名单。加入白名单后，Anti-DDoS 系统会再次回应 302 状态码，将客户端的访问重定向到一开始访问的 URI。后续这个客户端发出的 HTTP 请求报文命中白名单直接通过。

我们结合一组抓包信息来看一下交互报文的具体情况。

① Anti-DDoS 系统代替 Web 服务器与客户端建立 TCP 三次握手，然后客户端发起访问请求，如图 3-12 所示。

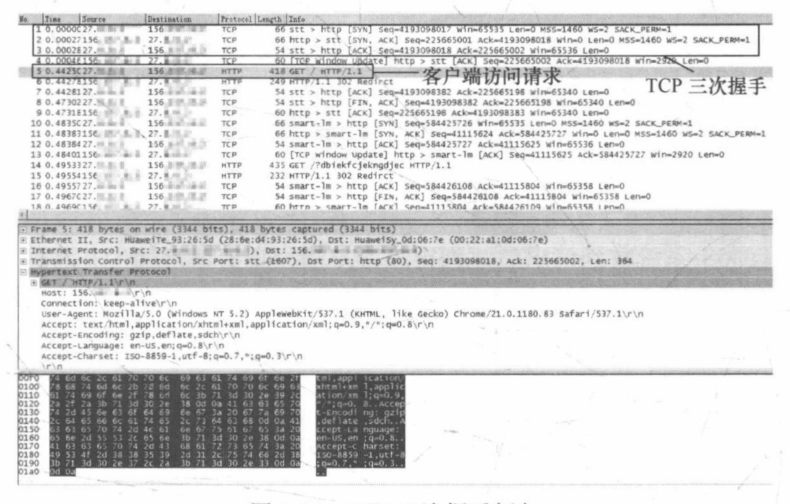


图 3-12 TCP 三次握手抓包

② Anti-DDoS 系统代替 Web 服务器回应 302 状态码，希望客户端访问一个新的 URI 地址“http://156***/?dbiekfcjekngdjec”，然后双方关闭连接，如图 3-13 所示。

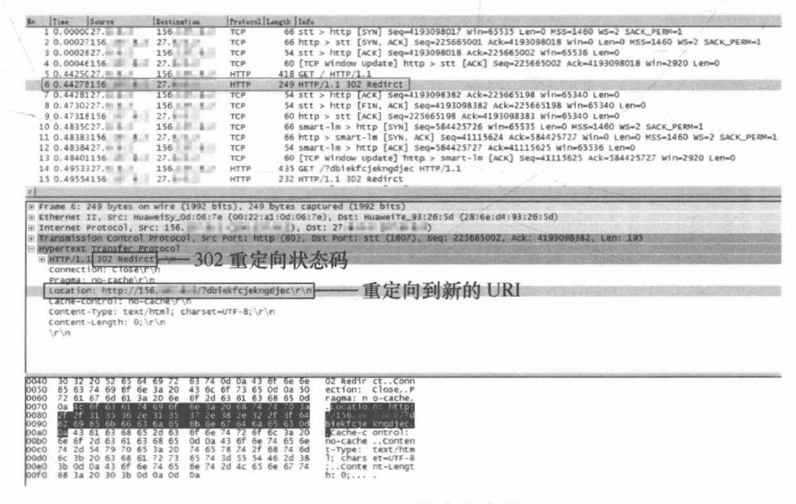


图 3-13 302 状态码抓包

③ 真实客户端会再次与 Anti-DDoS 系统建立 TCP 三次握手，并向新的 URI "http://156***/?dbiekfcjekngdjec" 发起请求，如图 3-14 所示。

再次建立 TCP 三次握手

客户端访问新的 URI

图 3-14 重新建立 TCP 三次握手抓包

④ Anti-DDoS 系统收到请求后，判定该客户端为真实客户端，并将其 IP 地址加入白名单。Anti-DDoS 系统会再次回应 302 状态码，将客户端的访问重定向到一开始访问的 URI，然后双方关闭连接，如图 3-15 所示。该客户端再发出 HTTP 请求报文就可以命中白名单直接通过了。

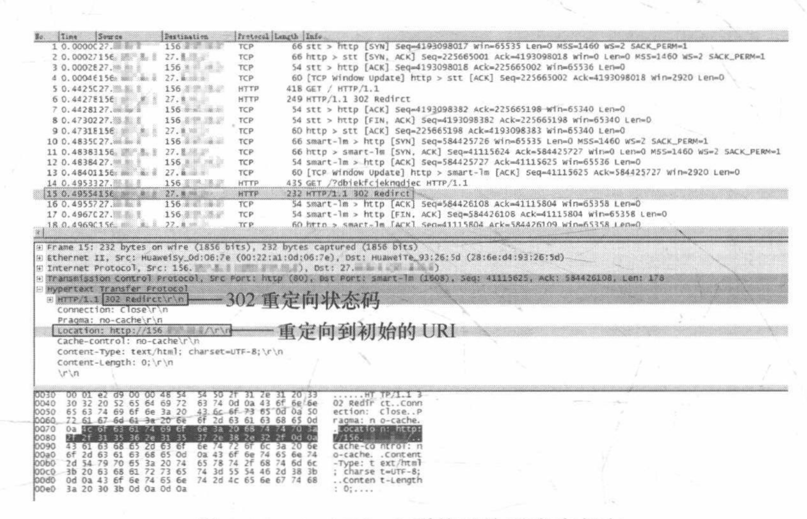


图 3-15 Anti-DDoS 系统再次重定向抓包

除了 302 状态码重定向方式，还有一种 META Refresh 重定向方式。META Refresh 方式是通过修改 HTML 页面来实现重定向，具有局限性；302 状态码方式是利用 HTTP 规范来实现重定向，适用性更好。因此 302 状态码方式是目前使用比较广泛的重定向方式。

另外还有一种情况，网络中存在 HTTP 代理服务器时，只要代理服务器 IP 地址通过源认证加入白名单，僵尸主机就可以利用代理服务器 IP 地址绕开源认证，导致防御失效。

针对这种情况，Anti-DDoS 系统提供了代理检测功能。开启该功能后，Anti-DDoS 系统会检测 HTTP 请求是不是通过代理服务器发出的。如果是，Anti-DDoS 系统会从 HTTP 报文中获取请求者的实际 IP 地址进行源认证，通过认证后才加入白名单。

302 重定向认证利用 HTTP 响应报文中的 302 状态码来实现对客户端的源认证功能，但是如果攻击工具实现了完整的 HTTP，或者像 H 站攻击事件中攻击源都是真实的浏览器这种情况，会导致 302 重定向认证方式失效。此时，Anti-DDoS 可以使用源认证中的增强方式，即验证码认证。

3.3.2 验证码认证

验证码认证的原理是 Anti-DDoS 系统要求客户端输入验证码，以此来判断请求是否由真实的用户发起，而不是由攻击工具或僵尸主机发起，如图 3-16 所示。因为攻击工具或僵尸主机无法自动响应随机变化的验证码，所以能够有效地防御攻击。

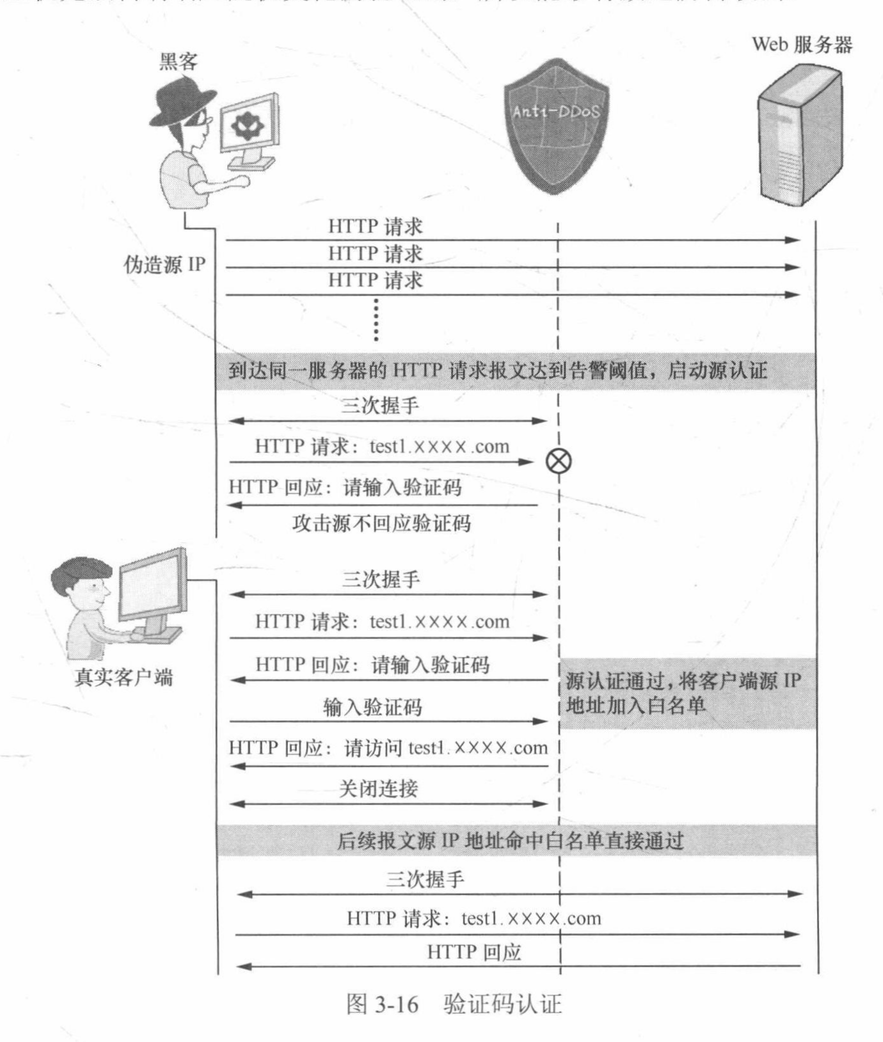


图 3-16 验证码认证

验证码认证过程如下。

① 当连续一段时间内去往目标 Web 服务器的 HTTP GET 请求报文超过告警阈

值后，Anti-DDoS 系统启动源认证机制。源认证机制启动后，Anti-DDoS 系统将会代替 Web 服务器与客户端建立 TCP 三次握手。

② Anti-DDoS 系统拦截 HTTP 请求，向客户端返回验证码页面，要求客户端输入验证码。

③ 如果这个源是攻击工具或僵尸主机，就不会输入验证码。

④ 如果这个源是真实客户端，就会输入验证码并通过认证，Anti-DDoS 系统将该客户端的源 IP 地址加入白名单。加入白名单后，Anti-DDoS 系统会请客户端继续访问一开始的 URI。

⑤ 后续这个客户端发出的 HTTP 请求报文命中白名单直接通过。

图 3-17 为 Anti-DDoS 系统向客户端返回的验证码页面的报文，以及对应的实际页面。

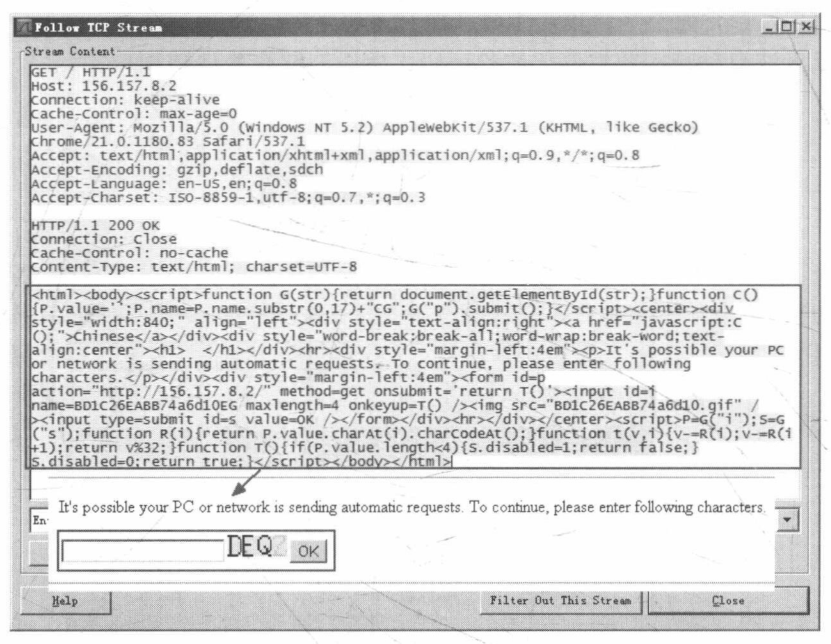


图 3-17 验证码页面

验证码认证方式与 302 认证方式相比，其防御效果更好，但是需要人手动输入验证码，用户体验稍差一些。我们在实际使用验证码认证方式时，可以增加源 IP 统计的环节，即 Anti-DDoS 系统先基于目的 IP 进行统计，当去往某个目的 IP 的 HTTP 请求超过阈值时，启动基于源 IP 的统计。当来自某个源的 HTTP 请求也超过阈值时，才启动验证码认证机制。这样就会精确控制需要进行验证码认证的源 IP 范围，避免大范围的源 IP 都要输入验证码。

302 重定向认证和验证码认证这两种源认证方式是防御 HTTP GET Flood 攻击的有效手段，但是源认证方式也存在一定的局限，比如机顶盒视频点播、特定移动网络等场景中，无法对客户端使用源认证方式。为此，Anti-DDoS 系统还支持 URI 动态指纹学习和 URI 行为监测防御方式，它们作为源认证方式的补充，满足不同场景的需求。

3.3.3 URI 动态指纹学习

URI 动态指纹学习方式适用于攻击源访问的 URI 比较固定的情况。要形成攻击

效果，攻击者一般都会以容易消耗系统资源的URI作为攻击目标。一个攻击源会发出多个针对该URI的请求，最终呈现为该源对特定的URI发送大量的请求报文。

基于这个原理，Anti-DDoS系统对客户端所访问的URI进行指纹学习，并找到攻击目标URI指纹。在一定的周期内，同一个源发出的包含同一指纹的请求超过设置的阈值时，就将该源加入黑名单。

3.3.4 URI行为监测

URI行为监测防御方式要先设置需要重点监测的URI，这样可以将消耗资源多、容易受到攻击的URI加入到“重点监测URI”列表中。URI行为监测防御方式通过判断两个比例是否超过阈值来确定攻击源。

在特定时间内，我们对所有客户端向某个目的服务器的所有访问中进行统计时发现，重点监测URI的访问数与总访问数的比例超过设置的阈值时，Anti-DDoS系统启动针对源的URI检测。当这个源对某个重点检测URI的访问数与总访问数的比例超过设置的阈值时，就将该源加入黑名单。

3.4 HTTP POST Flood攻击与防御

攻击者利用攻击工具或者操纵僵尸主机，向目标服务器发起大量的HTTP POST报文，消耗服务器资源，使服务器无法响应正常请求，这就是HTTP POST Flood攻击。

华为Anti-DDoS系统防御HTTP POST Flood攻击与防御GET Flood攻击类似，常用手段也是源认证，包括重定向认证和验证码认证。

3.4.1 重定向认证

Anti-DDoS系统代替Web服务器向客户端响应307状态码（针对POST请求方法的重定向），同时向客户端的浏览器注入Cookie，客户端再次发起请求时会在HTTP报头上附加Cookie信息，Anti-DDoS系统通过验证Cookie信息的真实性来验证客户端的真伪，如图3-18所示。

重定向认证过程如下。

① 当连续一段时间内去往目标Web服务器的HTTP POST请求报文超过告警阈值后，Anti-DDoS系统启动源认证机制。源认证机制启动后，Anti-DDoS系统将会代替Web服务器与客户端建立TCP三次握手。

② Anti-DDoS系统拦截HTTP请求。该系统代替Web服务器回应307状态码，并在响应头部附加上由客户端IP生成的Cookie。

③ 如果这个源是虚假源，或者不支持完整HTTP的攻击工具，不会重新发起请求。

④ 如果这个源是真实客户端，Anti-DDoS系统生成的Cookie会写入到浏览器中，并且客户端会重新发起请求，请求头部就会带有该Cookie信息。Anti-DDoS系统收到请求后，验证Cookie是否正确，如果正确则将该客户端的源IP地址加入白名单。加入白名单后，Anti-DDoS系统会回应408状态码，表示请求超时，客户端重新发起访问。

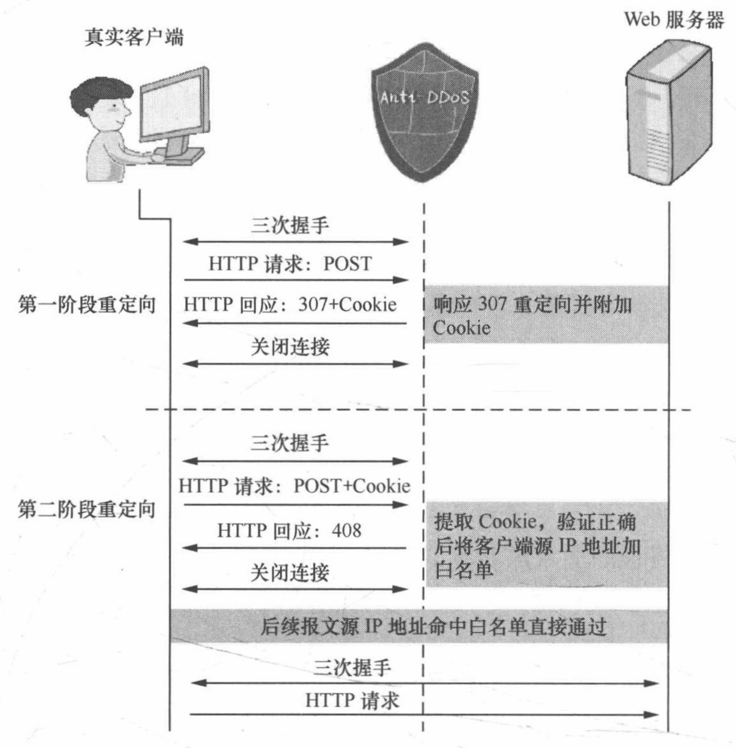


图 3-18 重定向认证

⑤ 后续这个客户端发出的 HTTP 请求报文命中白名单直接通过。

我们结合一组抓包信息来看一下交互报文的具体情况。

Anti-DDoS 系统代替 Web 服务器与客户端建立 TCP 三次握手，然后客户端发起访问请求，如图 3-19 所示。

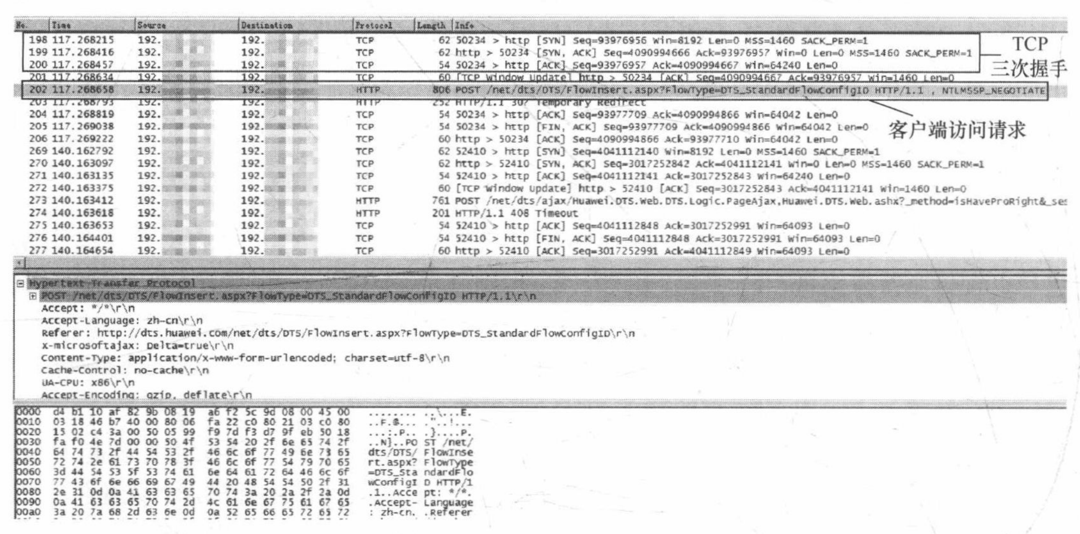


图 3-19 TCP 三次握手抓包

Anti-DDoS 系统代替 Web 服务器回应 307 状态码，同时在响应头部附加上由客户端

IP 生成的 Cookie，然后双方关闭连接，如图 3-20 所示。

图 3-20　Anti-DDoS 回应 307 状态码抓包

真实客户端会再次与 Anti-DDoS 系统建立 TCP 三次握手，并且会重新发起请求，请求头部就会带有 Cookie 信息，如图 3-21 所示。

图 3-21　重新建立 TCP 三次握手抓包

Anti-DDoS 系统收到请求后，其通过验证 Cookie 来判定该客户端为真实客户端，将其 IP 地址加入白名单。加入白名单后，Anti-DDoS 系统会回应 408 状态码，表示请求超时，客户端重新发起访问，如图 3-22 所示。

我们在上文中介绍的 307 重定向认证方式能够很好地防御 HTTP POST Flood 攻击，但是这种方式也具有局限性：其一，依赖于客户端浏览器的 Cookie 的机制，受安全级别限制。

如果客户端的浏览器安全级别较高而无法写入 Cookie，会导致认证不通过；其二，第一阶段重定向结束后，客户端需要被再次手动执行、提交等操作，才能重新发起 POST 请求。

408 请求超时状态码

图 3-22　Anti-DDoS 回应 408 状态码抓包

同 HTTP GET Flood 的防御方式相似，HTTP POST Flood 的源认证防御也支持增强方式，即验证码认证。

3.4.2　验证码认证

此处的验证码认证与 HTTP GET Flood 中的验证码机制相同，Anti-DDoS 系统要求客户端输入验证码，以此来判断请求是否由真实的用户发起。其弊端也是需要人手动输入验证码，用户体验稍差一些。具体的工作原理请参考 HTTP GET Flood 攻击与防御部分中的介绍，此处不再赘述。

3.4.3　URI 动态指纹学习和 URI 行为监测

我们在防御 HTTP POST Flood 攻击时，也可以使用 URI 动态指纹学习和 URI 行为监测防御方式，作为源认证方式的补充，满足不同场景的需求。其防御原理我们在上文的 HTTP GET Flood 攻击与防御部分已经介绍过，此处不再赘述。

了解两种 Flood 类攻击后，下面我们来介绍另外一种针对 HTTP 的 DDoS 攻击——慢速攻击。与 Flood 类攻击靠海量的数据洪流“淹没”目标服务器不同，慢速攻击反其道而行，它通过发送少量数据来维持连接状态，持续消耗目标服务器的资源。

3.5　HTTP 慢速攻击与防御

HTTP 慢速攻击是利用 HTTP 的正常交互机制，先与目标服务器建立一个连接，然后长时间保持该连接不释放。如果攻击者持续与目标服务器建立这样的连接，就会使目

标服务器上的可用资源耗尽，无法提供正常服务。

HTTP 慢速攻击主要包括针对 HTTP 请求报文头部结束符的 Slow Headers 攻击，以及针对 POST 请求报文数据长度的 Slow POST 攻击。

3.5.1　Slow Headers

我们在 HTTP 基础部分中介绍 HTTP 请求报文时，提到过请求头部的后面会存在一个空行（结束符），这其中包括回车符和换行符，客户端告知服务器请求头部结束，后面不再有请求头。如果服务器没有收到这个空行则会一直保持连接。

Slow Headers 攻击正是利用这一点，如图 3-23 所示，攻击者使用 GET 或 POST 请求方法与目标服务器建立连接，然后持续发送不包含结束符的 HTTP 头部报文，目标服务器会一直等待请求头部中的结束符，这导致连接始终被占用。攻击者控制大量的僵尸主机向目标服务器发起这种攻击，将会导致服务器资源耗尽，无法正常提供服务。

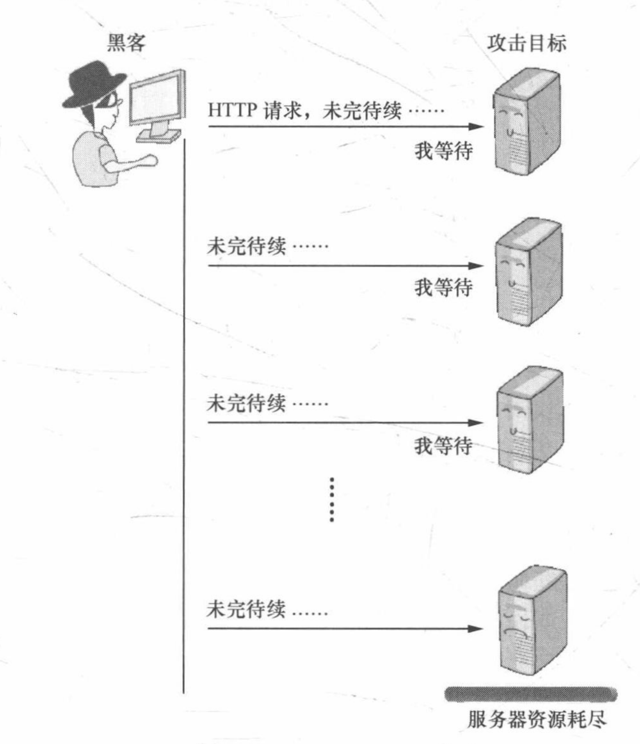


图 3-23　Slow Headers 攻击

如图 3-24 所示，正常的 HTTP 报文中请求头部的后面会有结束符 0x0d0a（\r\n 的十六进制表示方式），而攻击报文中不包含结束符，并且攻击者会持续发送不包含结束符的 HTTP 头部报文，维持连接状态，消耗目标服务器的资源。

Slow Headers 攻击行为的特征比较明显，华为 Anti-DDoS 系统防御 Slow Headers 攻击时，会对 HTTP 报文进行检查。如果发现某个源发出的连续多个 HTTP GET/POST 请求报文的报文头中都没有结束符（“\r\n”），则认为发生 Slow Headers 攻击，将该源 IP 地址加入黑名单。

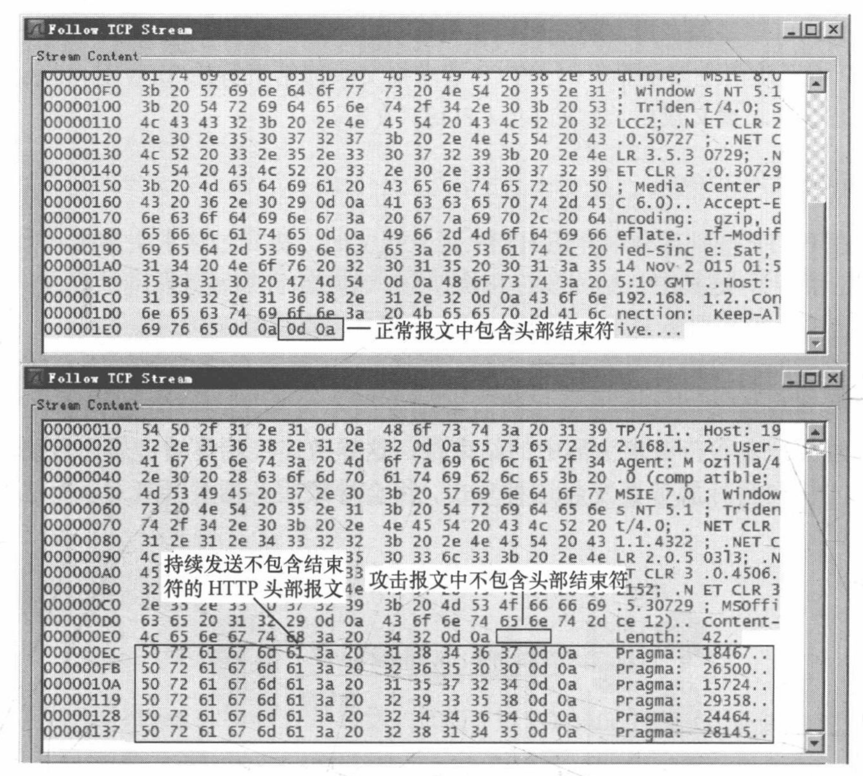


图 3-24 HTTP 报文中请求头

3.5.2 Slow POST

Slow POST 攻击利用的是 POST 请求方法，如图 3-25 所示，攻击者向目标服务器发送 POST 请求报文提交数据，数据的长度设置为一个很大的数值，但是在随后的数据发送中，每次只发送很小的报文，这就会导致目标服务器一直等待攻击者继续发送后续数据。攻击者控制大量的僵尸主机向目标服务器发起这种攻击，将会导致服务器资源耗尽，无法正常提供服务。

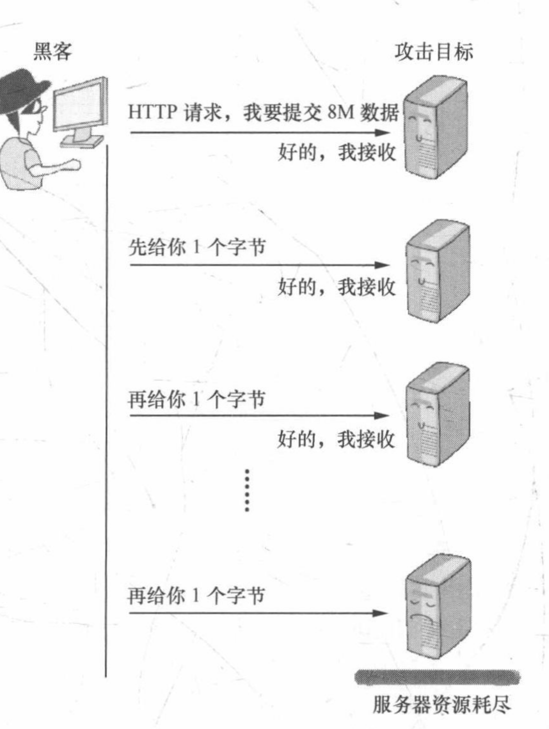


图 3-25 Slow POST 攻击

如图 3-26 所示，Slow POST 攻击报文中，POST 请求头部的 Content-Length 关键字的值设置为 8192，表示数据长度为 8192Byte。攻击者后续每次只发送 1 个字节的报文，导致连接一直被占用，消耗了服务器的资源。

华为 Anti-DDoS 系统防御 Slow POST 攻击时，防御方法也是对 HTTP 报文进行

检查。如果发现某个源发出的连续多个 HTTP POST 请求报文的长度值设置得很大，但是实际报文的数据部分长度值都很小，则认为发生 Slow POST 攻击，将该源 IP 地址加入黑名单。

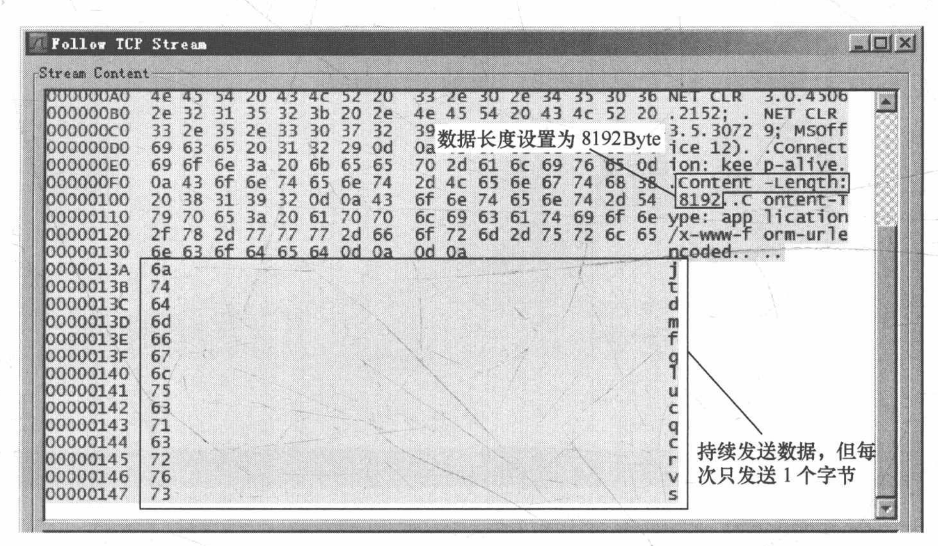
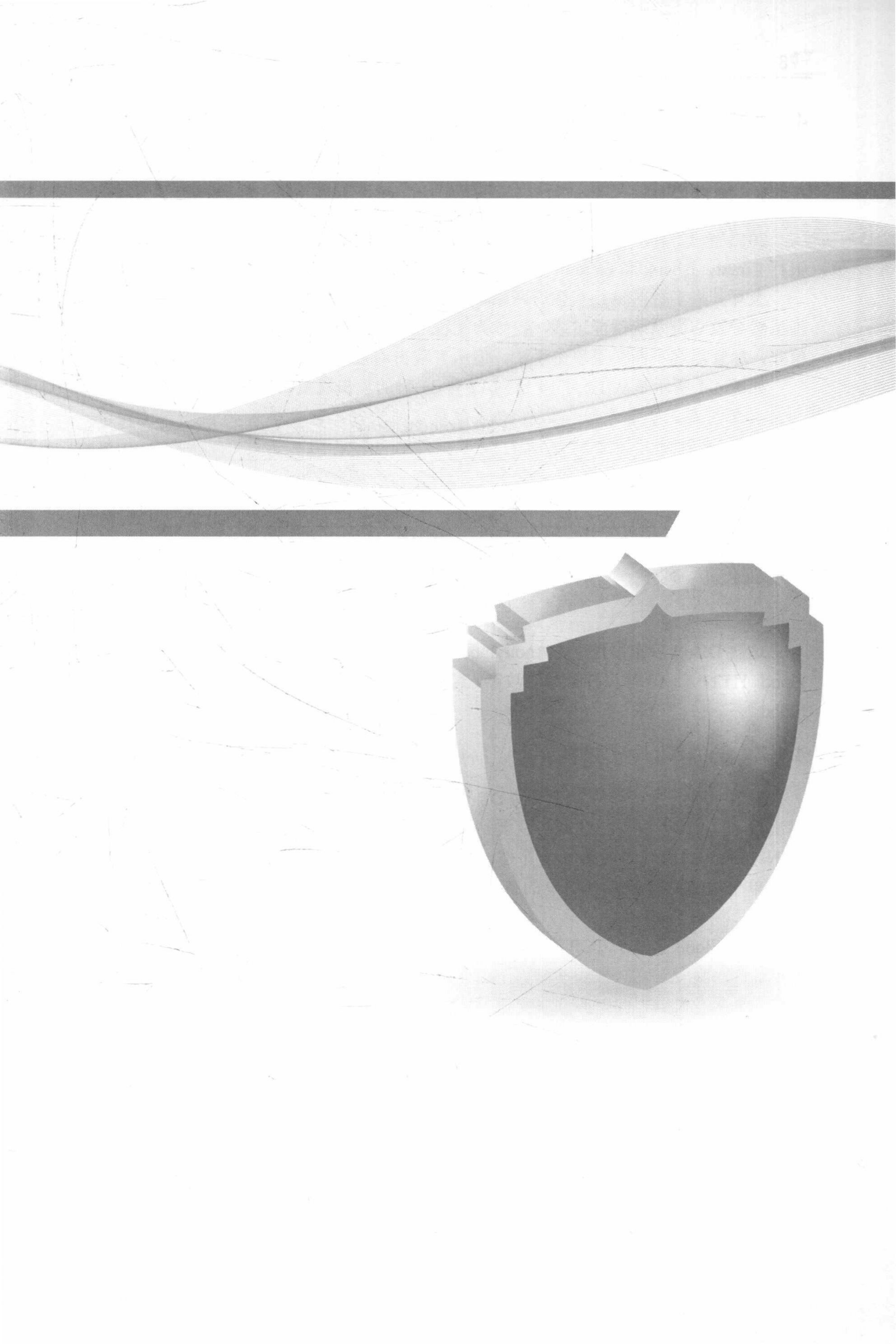


图 3-26　POST 请求头

第4篇 TCP



4.1 热点事件解密之：SYN Flood 攻击事件

4.1.1 事件回顾

2015 年 12 月，土耳其互联网遭遇了史上最大规模的 DDoS 攻击。土耳其三家知名银行 Ziraat、Isbank 和 Garanti 受到 DDoS 攻击，攻击流量峰值带宽高达 40Gbit/s。

土耳其大多数的银行和政府网站都在华为 Anti-DDoS 系统防御保护之中，大流量攻击虽然导致防御系统性能过载，但华为工程师现场紧急扩容板卡，研发远程 7×24 小时值守，尽管黑客不断变更攻击手法，但所有攻击均被成功阻断，网站访问正常。

如图 4-1 所示是从 12 月 14 日到 12 月 31 日的攻击流量峰值带宽。



图 4-1 攻击报表展示

这次 DDoS 攻击事件中，Anonymous 发动了混合型的攻击，包含 SYN Flood、UDP Flood、HTTP Flood 等多种类型的攻击，其中以 SYN Flood 为主，下面我们着重讲解 SYN Flood。

4.1.2 SYN Flood 攻击

SYN Flood 是互联网上经典的 DDoS 攻击方式之一，也是最原始的 DDoS 攻击，最早出现于 1999 年前后。在网络发展初期，由于系统的限制以及硬件资源性能的落后，SYN Flood 的出现对网络安全界是一大冲击。它与当时的单包攻击不同，工程师很难通过单个报文的特征或者简单的统计限流进行防御，每个报文看起来都是一个正常的报文。

SYN Flood 是基于 TCP 产生，其通过 TCP 的三次握手机制，攻击服务器，如图 4-2 所示。



图 4-2 TCP 三次握手

SYN Flood 三次握手时制造多个半连接，以此消耗服务器的连接数，如图 4-3 所示。

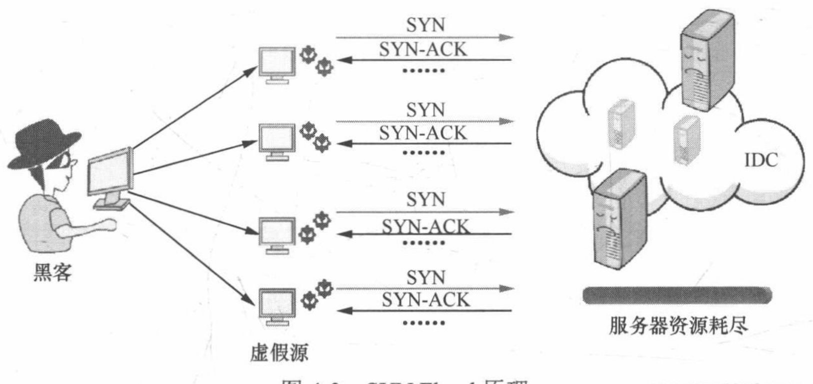


图 4-3 SYN Flood 原理

黑客伪造源 IP 地址向服务器发送大量的 SYN 报文，请求建立三次握手。由于发送源 IP 是伪造的，因此在服务器回应了一个 SYN-ACK 报文后，源 IP 并不会继续回应 ACK 报文进行确认。这时服务器会建立一个庞大的等待列表，不停地重复发送 SYN-ACK 报文，同时服务器占用着大量的资源无法释放。这导致被攻击的服务器被恶意半连接占满，不再接收新的 SYN 请求，而合法用户却无法完成三次握手去建立 TCP 连接。

比如，超市收银台被客户包围，但没有客户进行结账，收银台无法正常工作，这种是半连接。长此以往，超市瘫痪，资源耗尽，如图 4-4 所示。



图 4-4 超市收银被恶意霸占

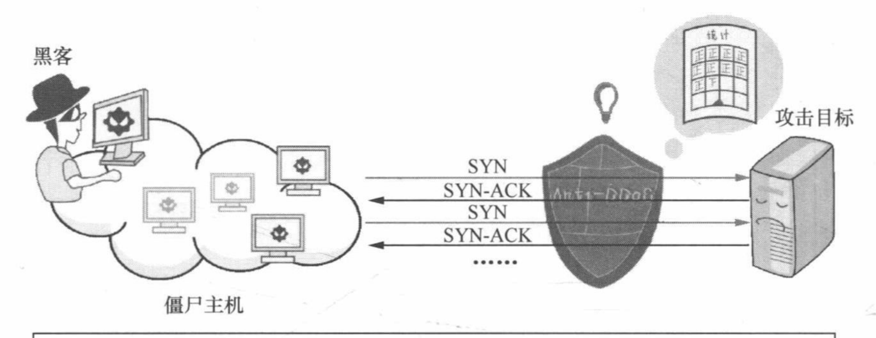
4.1.3 华为 Anti-DDoS 系统的解决方案

SYN Flood 这种没有明显攻击特征的报文，工程师不能通过特征识别或者指纹学习的方式对 SYN 报文进行过滤。我们可以从 SYN 报文建立连接的“行为”入手，判定其是否由真实源所发出的请求。

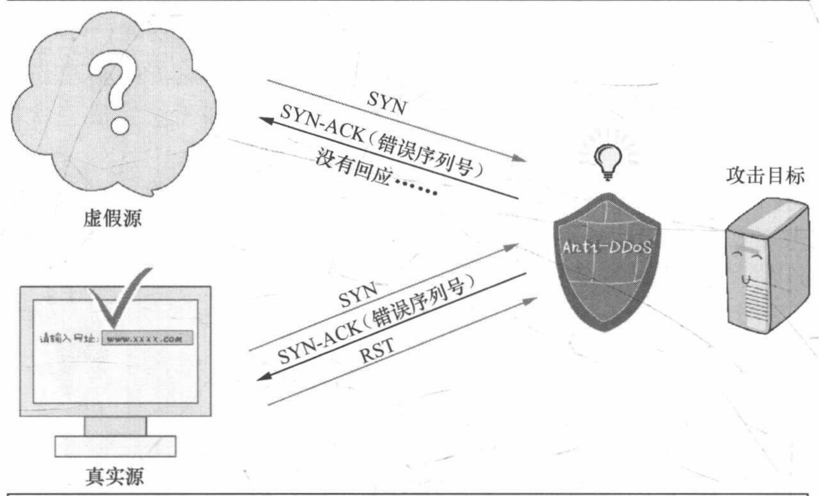
对于面向连接的 DDoS 攻击，最有效的防御方式是源认证。源认证有 3 个层面，分别为 TCP/IP 源认证、应用层源认证和用户源认证。

针对 SYN Flood 攻击的源认证，是整个源认证防御系统中的第一层 TCP/IP 源认证，如图 4-5 所示。在 TCP 三次握手还没有建立成功之前，Anti-DDoS 会验证攻击源的 TCP/IP 是否真实可信。

① 黑客控制僵尸主机用伪造源 IP 向服务器发起 SYN Flood 攻击，Anti-DDoS 对到达服务器的 SYN 报文进行统计，流量达到告警阈值后，触发防御机制



② 启动防御后，Anti-DDoS 拦截 SYN 报文，并反弹错误序列号的 SYN-ACK 到客户端。如果是虚假源，则不会响应 SYN-ACK 报文。如果是真实源，收到错误序列号的 SYN-ACK 报文后，会回应 RST 报文，要求重新建立连接



③ Anti-DDoS 将回应 RST 的客户端源 IP 加入白名单，并透传此客户端重新发送的 SYN 报文，客户端和服务器直接建立三次握手，并进行后续的数据传输

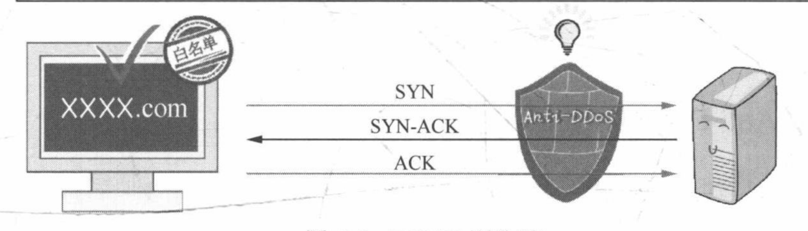


图 4-5 TCP/IP 源认证

从报文交互过程看出，Anti-DDoS 设备代替 Web 服务器向客户端反弹一个错误序列号的 SYN-ACK 报文，等待客户端的回应。

① 如果是虚假源，网络中不存在这个源 IP，或者源 IP 存在于网络但没有发送过 SYN 请求，源 IP 无故收到一个 SYN-ACK 报文，不会做任何响应，也无法通过源认证。

② 如果是真实源，当它收到一个错误的 SYN-ACK 报文，会回应一个 RST 报文，要求服务器重传。这时 Anti-DDoS 设备判定客户端是真实源，并加入白名单。后续这个源在一定时间内发送的 SYN 报文，会直接匹配白名单，并送达服务器。

当黑客发动 10GB 的变换源 IP 和源端口的攻击流量，服务器又反弹 10GB 的认证报文时，会造成网络严重拥塞。源认证的反弹机制会导致二次攻击的情况，因此 Anti-DDoS 设置了首包丢弃功能。

TCP 之所以可靠，除了三次握手机制，还有一个是处理数据超时和重传的机制，如图 4-6 所示。TCP 要求在发送端每发送一个报文段，就启动一个定时器并等待确认信息；接收端成功接收新数据后回复确认信息。若定时器在超时前数据未能被确认，TCP 会认为报文段中的数据已丢失或损坏，并对报文段中的数据进行重新组织和重传。

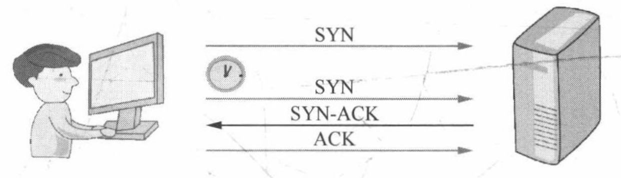


图 4-6　TCP 重传机制

首包丢弃便是利用 TCP 重传机制，对收到的第一个 SYN 报文直接丢弃，然后判定客户端是否重传。如果重传，再对第二个包进行源认证反弹。这样可以大大减少反弹包的数量，同时提高设备的处理性能，以达到最佳防御效果。

Anti-DDoS 设备判定这个报文是不是重传报文，有两个依据：三元组和时间间隔。三元组包含源 IP 地址、源端口和协议。

当 Anti-DDoS 设备收到一个 SYN 报文，首先会查询有没有匹配到三元组，如果没有，就认为该报文是首包，将其丢弃，并记录三元组信息。当 SYN 报文匹配到三元组时，再继续计算该报文与匹配到三元组的上一个报文到达的时间间隔。如果时间间隔不匹配，则认为是首包，将其丢弃；如果时间间隔匹配，则认为是后续包，将其放行。

源认证要和首包丢弃功能一起配合使用，对于虚假源攻击，尤其是针对不断变换源 IP 和源端口的虚假源攻击，可以达到最佳防御效果。其中，源认证是对 IP 层面的校验，认证这个源是不是真实存在的源；首包丢弃是对于 TCP 栈层面的校验，用于判断是否是这个源发出的真实请求。

4.2　TCP 解析

TCP 是每一位网络工程师在入门时学到的第一个协议。由于 TCP 的优良品质（面向连接、超时重传等可靠性保证），这个传输层协议构建了网络的半壁江山，很多常用的协议或应用如 Web、Telnet/SSH、FTP 等都是承载于 TCP。

我们以一次 FTP 连接建立和断开的过程为例，分析 TCP 报文的交互过程，了解 TCP 报文中的关键字段。图 4-7 为使用 Wireshark 工具中 Flow Graph 功能绘制出的整个交互过程的流程图，我们重点关注交互过程的一头一尾，即三次握手建立连接以及四次握手断开连接的过程。

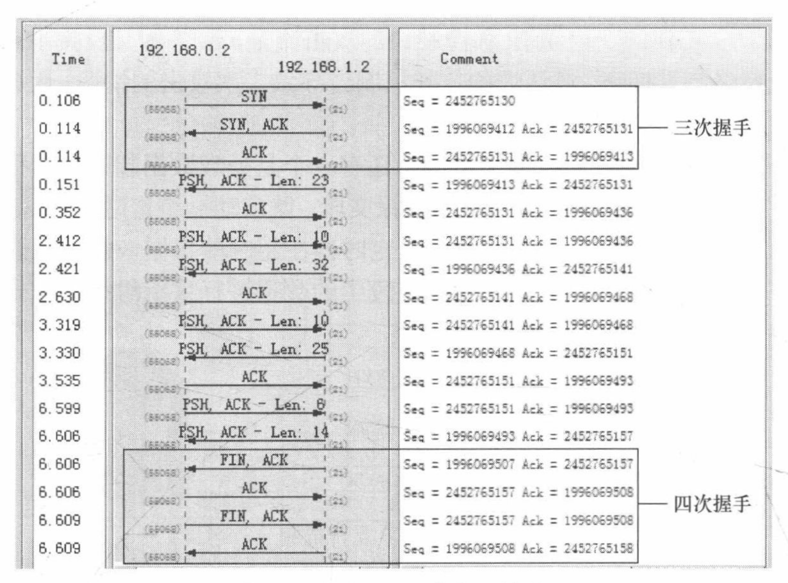


图 4-7　TCP 的整个交互过程

4.2.1　三次握手建立连接

在 TCP 中，通信双方使用三次握手来建立一个连接。

第一次握手时，客户端向服务器发起请求，报文中的 SYN 标志位置为 1，序号为 2452765130（用 X 标记），如图 4-8 所示。

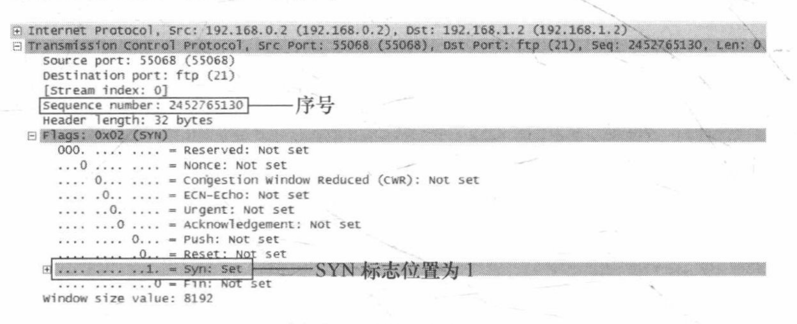


图 4-8　第一次握手

第二次握手时，服务器收到客户端的请求后，向客户端回应报文。报文中的 SYN 和 ACK 标志位均置为 1，序号为 1996069412（用 Y 标记），确认序号为客户端的序号+1，即 X+1=2452765131，如图 4-9 所示。

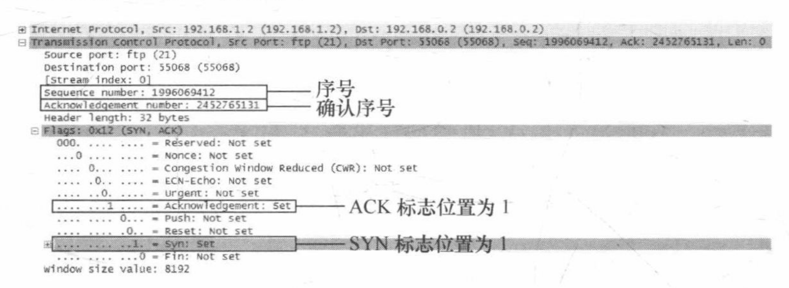


图 4-9　第二次握手

第三次握手时，客户端收到服务器回应的报文后，首先检查报文中的确认序号是否正确。如果确认序号正确（客户端的序号+1），即发送确认报文。确认报文中的 ACK 标志位置为 1，确认序号为服务器的序号+1，即 Y+1=1996069413，如图 4-10 所示。

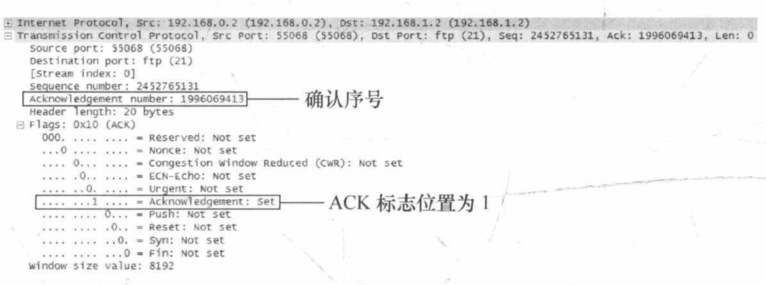


图 4-10 第三次握手

如果客户端检查服务器回应报文中的确认序号不正确，就会发送 RST（Reset 复位报文），报文中的 RST 标志位置为 1，表示连接出现问题，需要重新建立连接。

经过上述三次握手的交互过程，通信双方的一个 TCP 连接就建立完成了。

4.2.2 四次握手交互

由于 TCP 连接的全双工特性（两个方向能同时传输数据），因此通信双方断开一个连接需要经过四次握手的交互过程，或者称为四次挥手，意为双方向对方挥手告别。

由服务器发起断开连接的第一次握手，服务器要关闭与客户端的连接，服务器发送的报文中 FIN 标志位和 ACK 标志位均置为 1，序号为 1996069507（用 X 标记），如图 4-11 所示。

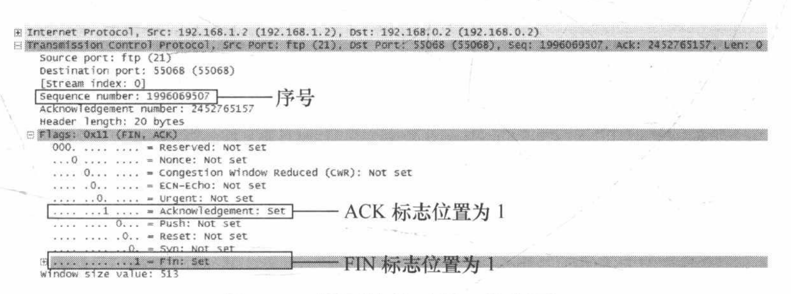


图 4-11 断开连接时第一次握手

第二次握手时，客户端收到服务器的 FIN 报文后，向服务器回应报文。报文中的 ACK 标志位置为 1，确认序号为客户端的序号+1，即 X+1=1996069508，如图 4-12 所示。

第三次握手时，客户端要关闭与服务器的连接，客户端发送的报文中，FIN 标志位和 ACK 标志位均置为 1，序号为 2452765157（用 Z 标记），如图 4-13 所示。

```
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.1.2 (192.168.1.2)
⊟ Transmission Control Protocol, Src Port: 55068 (55068), Dst Port: ftp (21), Seq: 2452765157, Ack: 1996069508, Len: 0
    Source port: 55068 (55068)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 2452765157
    Acknowledgement number: 1996069508 ——— 确认序号
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgement: Set ——— ACK 标志位置为 1
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 8098
```

图 4-12　断开连接时第二次握手

```
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.1.2 (192.168.1.2)
⊟ Transmission Control Protocol, Src Port: 55068 (55068), Dst Port: ftp (21), Seq: 2452765157, Ack: 1996069508, Len: 0
    Source port: 55068 (55068)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 2452765157 ——— 序号
    Acknowledgement number: 1996069508
    Header length: 20 bytes
  ⊟ Flags: 0x11 (FIN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgement: Set ——— ACK 标志位置为 1
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
    ⊞ .... .... ...1 = Fin: Set ——— FIN 标志位置为 1
    Window size value: 8098
```

图 4-13　断开连接时第三次握手

第四次握手时，服务器收到客户端的 FIN 报文后，向客户端回应报文。报文中的 ACK 标志位置为 1，确认序号为客户端的序号+1，即 Z+1=2452765158，如图 4-14 所示。

```
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.0.2 (192.168.0.2)
⊟ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 55068 (55068), Seq: 1996069508, Ack: 2452765158, Len: 0
    Source port: ftp (21)
    Destination port: 55068 (55068)
    [Stream index: 0]
    Sequence number: 1996069508
    Acknowledgement number: 2452765158 ——— 确认序号
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgement: Set ——— ACK 标志位置为 1
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 513
```

图 4-14　断开连接时第四次握手

经过上述四次握手的交互过程，通信双方断开了一个 TCP 连接。

综上所述，TCP 连接建立和断开过程涉及很多概念。首先，TCP 报文的类型有很多种，包括 SYN、ACK、FIN 以及 RST 等，不同类型的报文各司其职；其次，TCP 报文的内容比较复杂，除了 IP 地址和端口之外，还包括序号、确认序号、各种标志位等。

攻击者会利用交互过程来对 TCP 进行攻击，可能使用的攻击方式有以下几种。

（1）Flood 类攻击

例如，攻击者向攻击目标发送海量的 SYN、ACK、FIN 或 RST 报文，占用被攻击目标的系统资源，使其无法提供正常服务。

（2）连接耗尽类攻击

例如，攻击者与被攻击目标完成三次握手后不再发送报文但一直维持连接，或者立刻发送 FIN 或 RST 报文，在断开连接后快速发起新的连接等，消耗 TCP 连接资源。

（3）异常报文类攻击

例如，TCP 报文中的标志位全都置为 1 或 0，SYN 和 FIN 标志位同时置为 1 等，这些不符合 TCP 规范的异常报文可能会导致被攻击目标的系统崩溃。

4.3 SYN Flood 攻击与防御

SYN Flood 指的是攻击者利用工具或者操作僵尸主机，向目标服务器发起大量的 TCP SYN 报文，当服务器回应 SYN-ACK 报文时，攻击者不再继续回应 ACK 报文。这时服务器上存在大量的 TCP 半连接，服务器的资源会被这些半连接耗尽，无法响应正常的请求。

华为 Anti-DDoS 解决方案防御 SYN Flood 攻击的常用方式是源认证，从 SYN 报文建立连接的“行为”入手，判断是否为真实源发出的请求。源认证包括基本源认证和高级源认证，下面我们将介绍这两种认证方式。

4.3.1 基本源认证

基本源认证的原理是 Anti-DDoS 系统代替 Web 服务器向客户端响应 SYN-ACK 报文，报文中带有错误的确认序号。当真实的客户端收到带有错误确认序号的 SYN-ACK 报文后，会向服务器发送 RST 报文，要求重新建立连接；而虚假源收到带有错误确认序号的 SYN-ACK 报文，不会做出任何响应。Anti-DDoS 系统通过观察客户端的响应情况，来判断客户端的真实性，如图 4-15 所示。

SYN Flood 基本源认证过程有以下 4 步。

① 当连续一段时间内去往目标服务器的 SYN 报文超过告警阈值后，Anti-DDoS 系统启动源认证机制。源认证机制启动后，Anti-DDoS 系统将会代替 Web 服务器向客户端响应带有错误确认序号的 SYN-ACK 报文。

② 如果是虚假源，是一个不存在的地址或者是存在的地址但却没有发送过 SYN 报文，其不会做出任何响应。

③ 如果是真实客户端，则会向服务器发送 RST 报文，并要求重新建立连接。Anti-DDoS 系统收到 RST 报文后，将该客户端的源 IP 地址加入白名单。

④ 后续真实客户端发出的 SYN 报文命中白名单直接通过。

基本源认证方式存在一定的局限性，如果网络中存在某些设备会丢弃带有错误确认序号的 SYN-ACK 报文，或者有的客户端不响应带有错误确认序号的 SYN-ACK 报文，基本源认证就不会生效。这时还可以使用高级源认证来验证客户端的真实性。

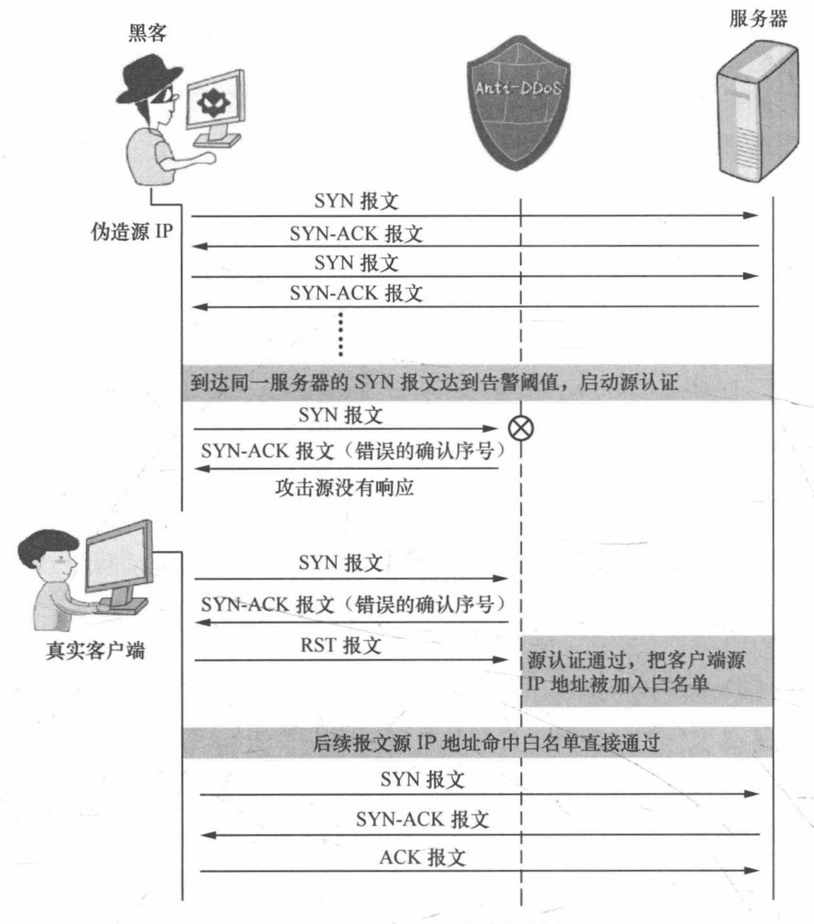


图 4-15 SYN Flood 基本源认证

4.3.2 高级源认证

高级源认证的原理也是 Anti-DDoS 系统代替 Web 服务器向客户端响应 SYN-ACK 报文，但与基本源认证不同的是，SYN-ACK 报文中带有正确的确认序号。真实的客户端收到带有正确确认序号的 SYN-ACK 报文后，它会向服务器发送 ACK 报文；而虚假源收到带有正确确认序号的 SYN-ACK 报文后，它不会做出任何响应。Anti-DDoS 系统通过观察客户端的响应情况，来判断客户端的真实性，如图 4-16 所示。

SYN Flood 高级源认证过程有以下 4 步。

① 当在连续一段时间内去往目标服务器的 SYN 报文超过告警阈值时，Anti-DDoS 系统启动源认证机制。源认证机制启动后，Anti-DDoS 系统将会代替 Web 服务器向客户端响应带有正确确认序号的 SYN-ACK 报文。

② 如果这个源是虚假源，是一个不存在的地址或者是存在的地址但却没有发送过 SYN 报文，其不会做出任何响应。

③ 如果这个源是真实客户端，其会向服务器发送 ACK 报文，并对收到的 SYN-ACK

报文进行确认。Anti-DDoS 系统收到 ACK 报文后，将该客户端的源 IP 地址加入白名单。同时，Anti-DDoS 系统会向客户端发送 RST 报文，要求重新建立连接。

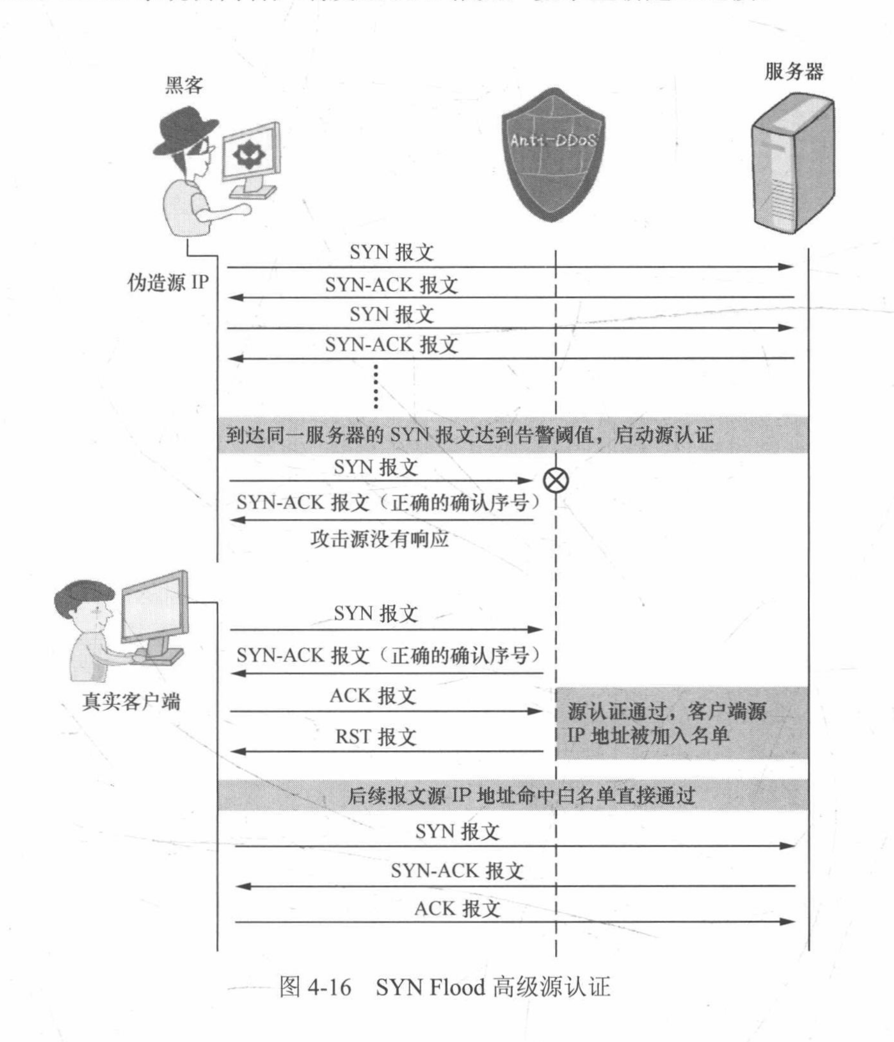


图 4-16　SYN Flood 高级源认证

④ 后续这个客户端发出的 SYN 报文命中白名单直接通过。

无论是基本源认证还是高级源认证，其原理都是 Anti-DDoS 系统发送 SYN-ACK 报文来对源进行认证。Anti-DDoS 系统收到 SYN 报文后会反弹 SYN-ACK 报文。如果网络中存在海量的 SYN 报文，同样 Anti-DDoS 系统也会反弹出去海量的 SYN-ACK 报文，这样势必会造成网络拥塞更加严重。

为了避免这个问题，减少反弹的 SYN-ACK 报文对网络拥塞的影响，Anti-DDoS 系统提供了首包丢弃功能。

4.3.3　首包丢弃

TCP 的可靠性保证了面向连接（三次/四次握手），还体现在超时与重传机制。TCP 规范要求发送端每发送一个报文，就启动一个定时器并等待确认信息；如果在定时器超时前还没有收到确认，就会重传报文。

首包丢弃功能就是利用了 TCP 的超时重传机制，Anti-DDoS 系统对收到的第一个 SYN 报文直接丢弃，然后观察客户端是否重传。如果客户端重传了 SYN 报文，再对重传的 SYN 报文进行源认证，即反弹 SYN-ACK 报文，这样就可以大大减少了反弹报文的数量，如图 4-17 所示。

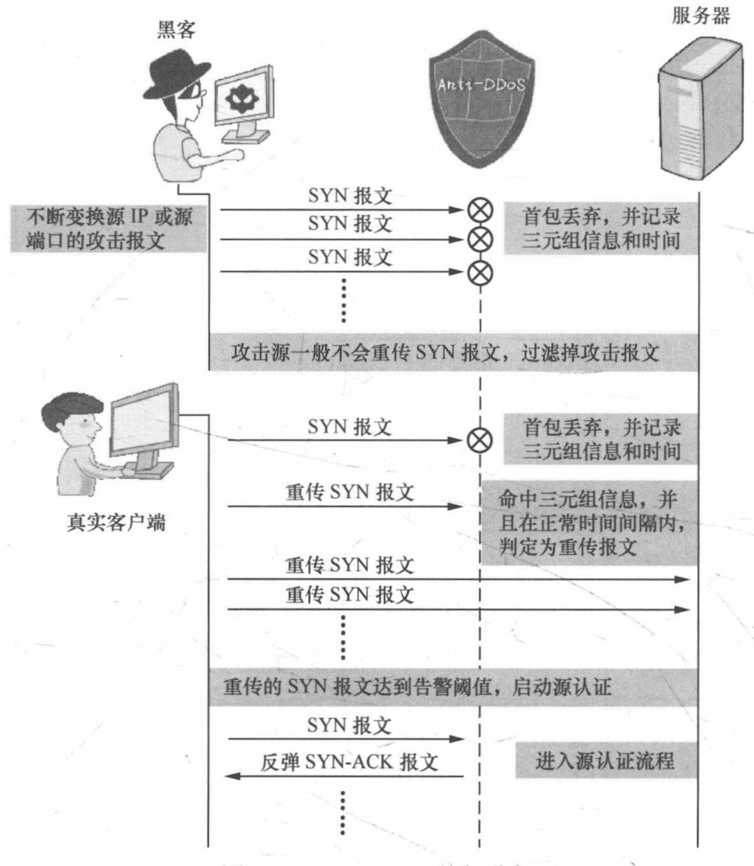


图 4-17　SYN Flood 首包丢弃

实际部署时，我们将首包丢弃和源认证结合使用。防御 SYN Flood 攻击时，先通过首包丢弃功能过滤一些攻击报文，当重传的 SYN 报文超过告警阈值后，再启动源认证。这样可以减少反弹的 SYN-ACK 报文的数量，缓解网络拥塞情况。对于虚假源攻击，尤其是对于不断变换源 IP 和源端口的虚假源攻击，可以达到最佳防御效果。

4.4　SYN-ACK&ACK&FIN&RST Flood 攻击与防御

除了 SYN 报文之外，TCP 交互过程中还存在 SYN-ACK、ACK、FIN 和 RST 报文，这几类报文也可能会被攻击者利用，海量的攻击报文会导致被攻击目标系统资源

耗尽、网络拥塞，无法正常提供服务。接下来我们介绍几种常见的 Flood 攻击的原理和防御方式。

4.4.1　SYN-ACK Flood 攻击与防御

通信双方通过三次握手建立一个 TCP 连接的过程时，SYN-ACK 报文出现在第二次握手中，是用来确认第一次握手的。一方收到 SYN-ACK 报文后，首先会判断该报文是不是属于三次握手范畴之内的报文。如果还在进行第一次握手便又收到了第二次握手的报文，向对方发送 RST 报文，告知对方其发来的报文有误，不能建立连接。

SYN-ACK Flood 攻击是攻击者利用工具或者操控僵尸主机，向目标服务器发送大量的 SYN-ACK 报文，这些报文都属于凭空出现的第二次握手报文，服务器忙于回复 RST 报文，导致资源耗尽，无法响应正常的请求。

华为 Anti-DDoS 解决方案使用源认证方式防御 SYN-ACK Flood 攻击，其原理是 Anti-DDoS 系统向发送 SYN-ACK 报文的源地址发送 SYN 报文，相当于发起了第一次握手，以探测该地址是否真实存在。如图 4-18 所示，真实的源会向 Anti-DDoS 系统响应正确的 SYN-ACK 报文，即第二次握手的报文；而虚假的源则不会响应正确的 SYN-ACK 报文。

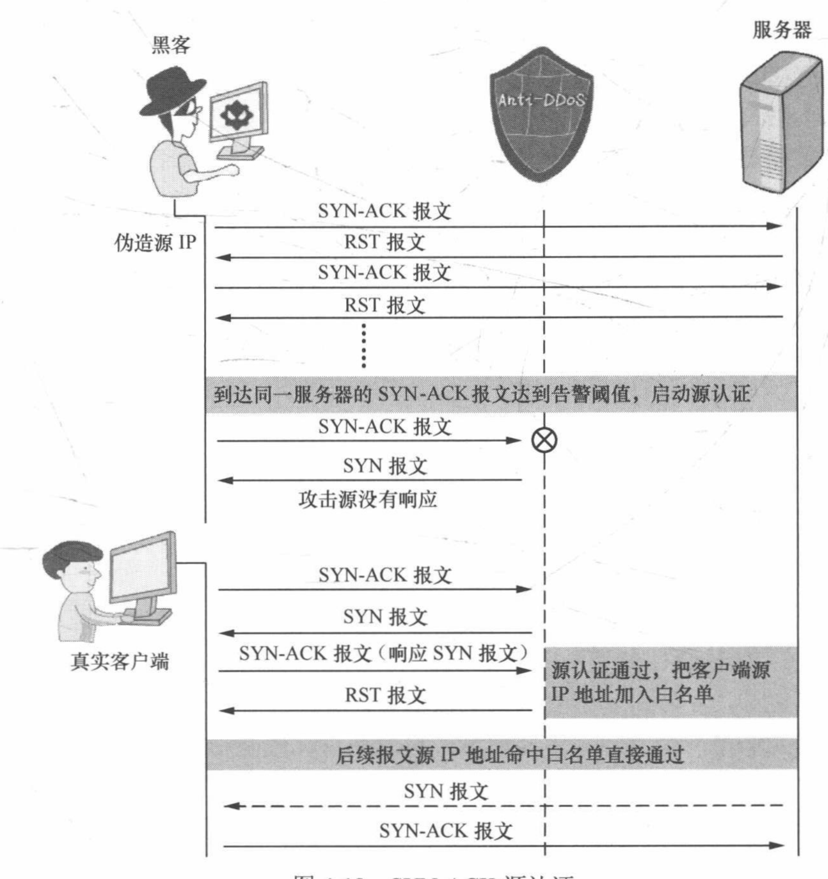


图 4-18　SYN-ACK 源认证

SYN-ACK Flood 源认证过程有以下 4 步。

① 在连续一段时间内去往目标服务器的 SYN-ACK 报文超过告警阈值后，Anti-DDoS 系统启动源认证机制。源认证机制启动后，Anti-DDoS 系统向发送 SYN-ACK 报文的源地址发送 SYN 报文。

② 如果这个源是虚假源，其不会向 Anti-DDoS 系统响应正确的 SYN-ACK 报文。

③ 如果这个源是真实源，其会向 Anti-DDoS 系统响应正确的 SYN-ACK 报文。Anti-DDoS 系统收到该 SYN-ACK 报文后，将该源 IP 地址加入白名单，同时会向源地址发送 RST 报文，断开自己和这个源地址的连接。

④ 后续这个源发出的 SYN-ACK 报文命中白名单直接通过，而对于那些未匹配白名单的 SYN-ACK 报文则继续进行源认证。

Anti-DDoS 系统防御 SYN-ACK Flood 攻击与防御 SYN Flood 攻击时所采用的方式类似，都是采用源认证的方式。

4.4.2 ACK Flood 攻击与防御

在 TCP 三次的握手过程中，ACK 报文出现在第三次握手时，用以确认第二次握手中的 SYN-ACK 报文。ACK Flood 攻击指的是攻击者利用工具或者操控僵尸主机，向目标服务器发送大量的 ACK 报文，服务器忙于回复这些凭空出现的第三次握手报文，导致资源耗尽，无法响应正常的请求。

华为 Anti-DDoS 解决方案使用会话检查的方式防御 ACK Flood 攻击，这与防御 SYN Flood 和防御 SYN-ACK Flood 时所采用的方式有所不同。会话是状态检测防火墙的一个机制，是防火墙最基本的功能，也是实现安全防护的基础技术。

Anti-DDoS 系统借鉴了防火墙的会话机制，其通过检查会话来确定 ACK 报文的真实性。我们可以把 Anti-DDoS 系统看作是关闭了链路状态检查功能的防火墙，SYN、SYN-ACK、ACK 等报文都会创建会话。一次正常的 TCP 连接建立过程，必须先有 SYN 报文，接着是 SYN-ACK 报文，然后才是 ACK 报文，所谓有“因”才有“果”。只有 ACK 报文命中了会话这个“因”，才能说明该报文是正常交互过程中的报文，是真实的报文。

Anti-DDoS 系统对 ACK 报文进行会话检查时，支持基本和严格两种模式，下面我们进行具体讲解。

1. 基本模式

使用基本模式时，Anti-DDoS 系统对 ACK 报文进行会话检查，如果 ACK 报文没有命中会话，Anti-DDoS 系统会允许第一个 ACK 报文通过，并建立会话，以此来对后续 ACK 报文进行会话检查；如果 ACK 报文命中了会话，则继续检查报文的序号，允许序号正确的报文通过，序号不正确的报文则被丢弃，如图 4-19 所示。

基本模式允许第一个 ACK 报文通过，检查条件比较宽松。如果攻击者发送变源或变端口的 ACK 报文，基本模式会允许报文通过并建立会话，这样会导致攻击报文被放过，影响防御效果。为此，Anti-DDoS 系统还提供了严格模式，检查条件更加严格，防御效果也会更好一些。

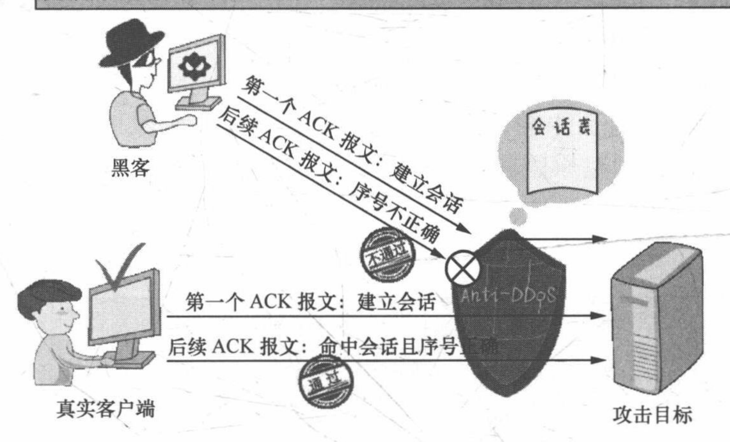


图 4-19 ACK Flood 基本模式

2. 严格模式

严格模式指的是 Anti-DDoS 系统对 ACK 报文进行会话检查时，如果 ACK 报文没有命中会话，系统直接丢弃报文；如果 ACK 报文命中会话，并且序号正确，系统允许报文通过，如图 4-20 所示。

严格模式的检查条件比较苛刻，没有命中会话的 ACK 报文都会被丢弃。在旁路部署动态引流的场景，由于报文来回路径不一致，正常业务的 ACK 报文会因为没有命中会话而被丢弃，因此对正常业务有一定的影响。

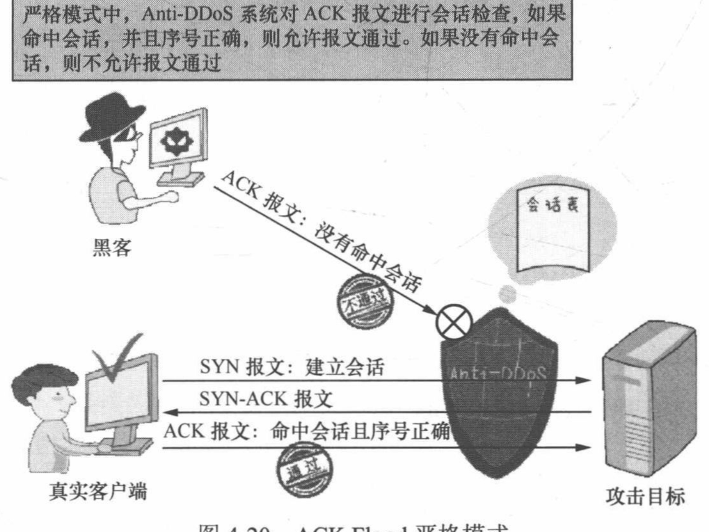


图 4-20 ACK Flood 严格模式

4.4.3 FIN/RST Flood 攻击与防御

TCP 交互过程中还存在 FIN 报文和 RST 报文，FIN 报文用来关闭 TCP 连接，RST 报文用来断开 TCP 连接。这两种报文也可能会被攻击者利用来发起 DDoS 攻击，导致目标服务器资源耗尽，无法响应正常的请求。

华为 Anti-DDoS 解决方案同样使用会话检查的方式防御 FIN/RST Flood 攻击。如果 FIN/RST 报文没有命中会话，系统直接丢弃报文；如果 FIN/RST 报文命中会话，系统则根据会话创建原因和会话检查结果来判断该报文是否通过，如图 4-21 所示。

Anti-DDoS 系统对 FIN/RST 报文进行会话检查，如果没有命中会话，则不允许报文通过。如果命中会话，再分为两种情况：会话是由 SYN 报文或 SYN-ACK 会话是由 SYN 或 SYN-ACK 报文创建的，允许报文通过；会话是由其他报文创建的，则允许序号正确的报文通过，不允许序号不正确的报文通过

图 4-21 FIN/RST Flood 会话检查

① 如果会话是由 SYN 报文或 SYN-ACK 报文创建的，则允许该 FIN/RST 报文通过。

② 如果会话是由其他报文创建的（例如 ACK 报文），则进一步检查报文序号是否正确，允许序号正确的报文通过，序号不正确的报文则被丢弃。

4.5 TCP 连接耗尽攻击&异常报文攻击与防御

4.5.1 TCP 连接耗尽攻击与防御

TCP 是面向连接的协议，其通信双方必须保持连接状态，并且通过确认、重传、滑动窗口等机制，保证数据传输的可靠性和稳定性。攻击者利用 TCP 的上述特点，利用 TCP 连接消耗被攻击目标的系统资源，这类攻击的影响也不容小觑。

例如，攻击者与被攻击目标完成三次握手后，立刻发送FIN报文或RST报文，释放本端连接，同时快速发起新的连接，以此来消耗被攻击目标的系统资源。华为Anti-DDoS解决方案通过检查新建连接的速率来防御此类攻击。首先，针对受保护目标进行统计，当受保护目标的TCP新建连接速率超过阈值时，启动防御功能。然后针对源进行统计，如果某个源IP在指定的时间间隔内发起的TCP新建连接数超过了阈值，则将该源IP加入黑名单，如图4-22所示。

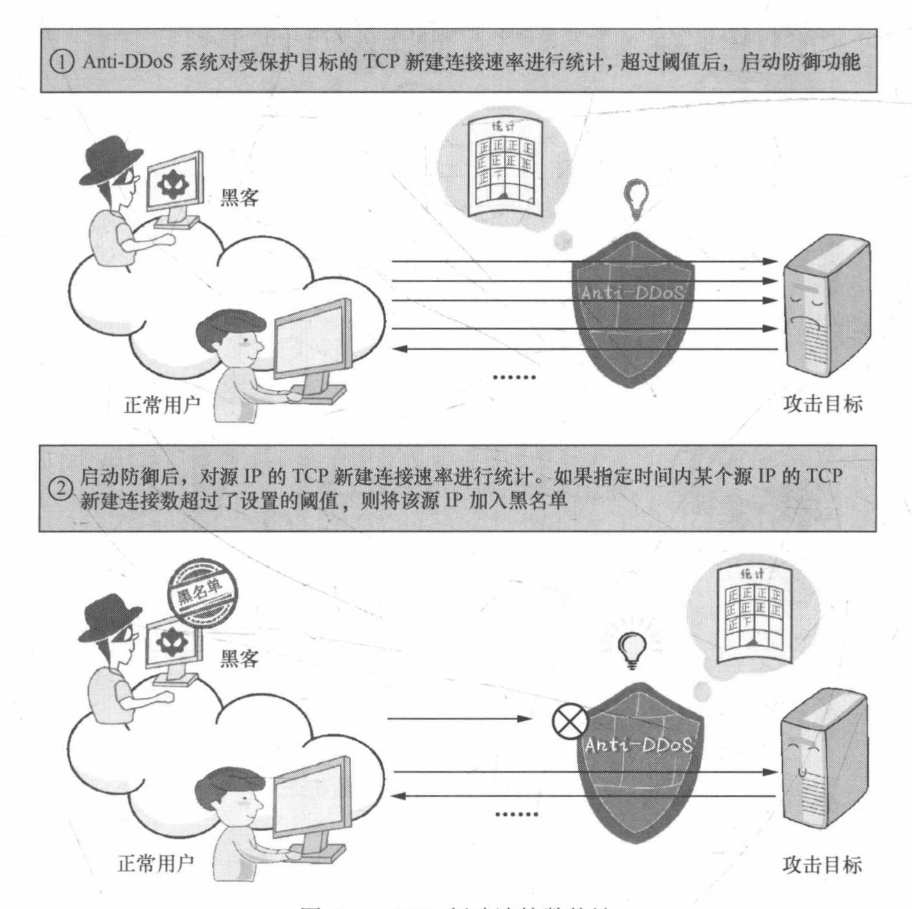


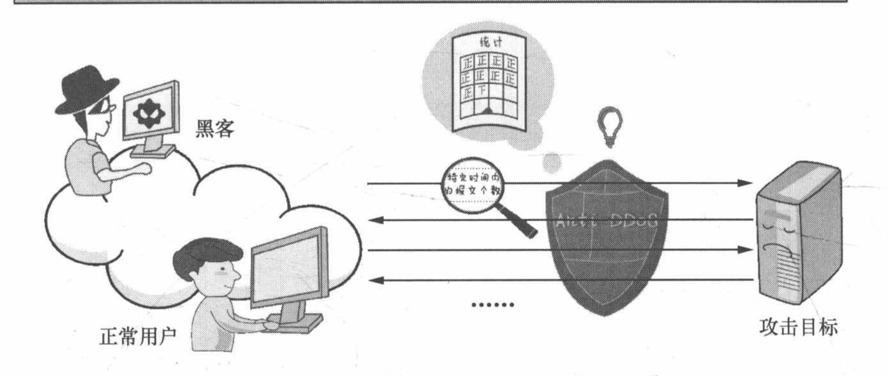
图4-22　TCP新建连接数统计

另外，攻击者与被攻击目标完成三次握手后，发送很少的报文来维持连接状态，通过这种异常的TCP连接来消耗被攻击目标的系统资源。华为Anti-DDoS解决方案通过异常会话检查来防御此类攻击。如果受保护目标的TCP连接上在特定时间内通过的报文数小于阈值，则认为该连接为异常会话。如果在特定时间内某个源IP的异常会话数超过阈值，则将该源IP加入黑名单，如图4-23所示。

除此之外，攻击者还会使用其他的攻击手段，比如构造大量的并发连接、设置很小的TCP窗口、发送重传报文等，其目的都是消耗被攻击目标的系统资源。总体来说，华为Anti-DDoS解决方案在防御此类攻击时，要基于会话机制，通过新建连接速率检查、

并发连接数检查、异常会话检查等措施，将攻击源加入黑名单，阻断攻击流量达到防御效果。

① Anti-DDoS 系统对受保护目标的 TCP 连接上的报文数进行检查，如果特定时间内通过的报文数小于阈值，判定为异常会话



② Anti-DDoS 系统对异常会话数进行统计。如果指定时间内某个源 IP 的异常会话数超过了设置的阈值，则将该源 IP 加入黑名单

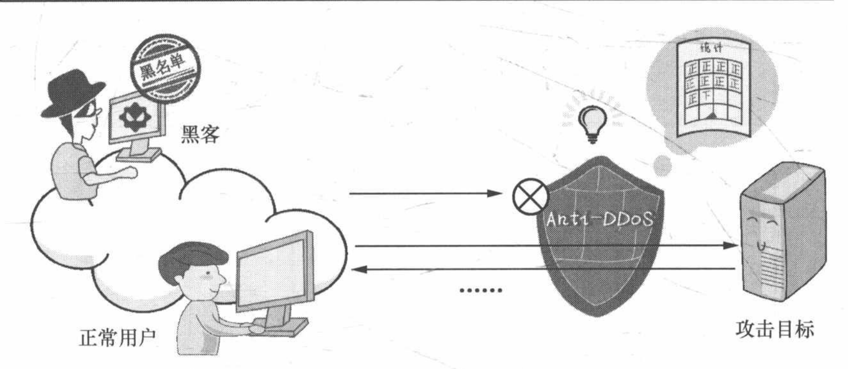


图 4-23　TCP 连接的报文数统计

4.5.2　TCP 异常报文攻击与防御

TCP 报文头中存在 6 个标志位字段，其代表不同的含义，标志位的值置为 1，表示该标志位起作用。我们在上文介绍 TCP 连接建立和断开过程时，提到过 SYN、ACK 和 FIN 标志位，下面是这 6 个标志位的详细信息。

① URG：置 1 时表示紧急指针有效。

② ACK：置 1 时表示确认序号有效。

③ PSH：置 1 时表示接收方收到数据段后应该尽快送到应用程序。

④ RST：置 1 时表示重新建立连接。

⑤ SYN：置 1 时表示发起一个连接。

⑥ FIN：置 1 时表示发送方完成发送任务，释放连接。

这 6 个标志位在 TCP 交互过程中各司其职，标志位置必须严格遵循 TCP 规范。如果不遵循规范随意将标志位置 0 或置 1，这类报文称为 TCP 异常报文。接收方处理这些异常报文时会消耗系统资源，甚至可能会导致系统崩溃。攻击者也可以利用 TCP 异常报文来发起 DDoS 攻击，向被攻击目标发送大量构造的 TCP 异常报文，导致被攻击目标系统资源耗尽、网络拥塞，无法正常提供服务。

华为 Anti-DDoS 解决方案通过检查 TCP 报文是否符合协议规范来防御异常报文攻击。例如，正常情况下 TCP 报文中六个标志位的值不可能都置为 0，当 Anti-DDoS 系统检查发现此类异常报文后，直接将报文丢弃，如图 4-24 所示。

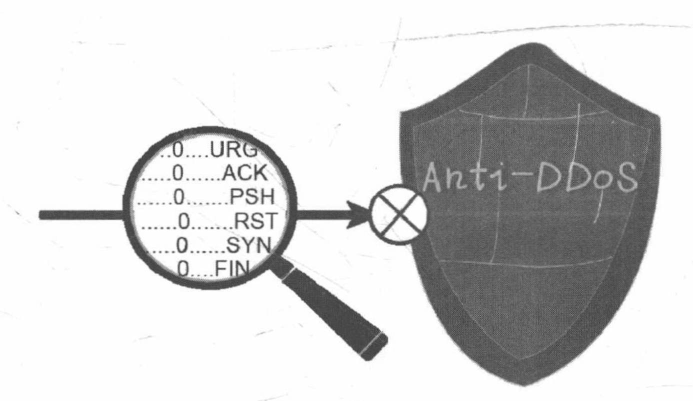


图 4-24 TCP 异常标志位检查

另外，SYN 标志位用来建立连接，FIN 标志位用来断开连接，正常情况下同一个 TCP 报文中 SYN 标志位和 FIN 标志位不可能同时置为 1。同样，Anti-DDoS 系统检查发现此类异常报文后，直接丢弃报文，如图 4-25 所示。

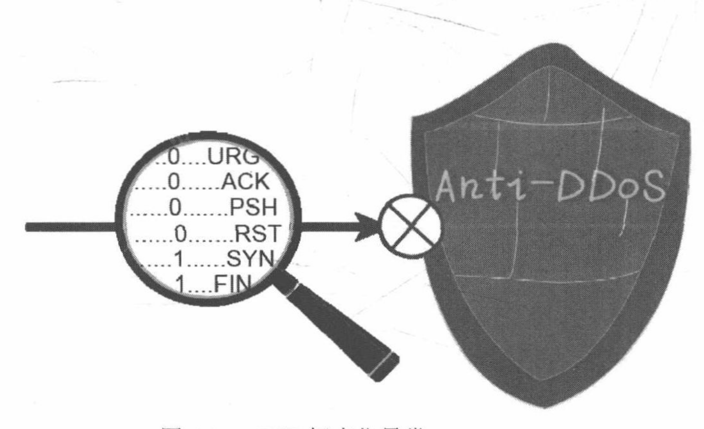
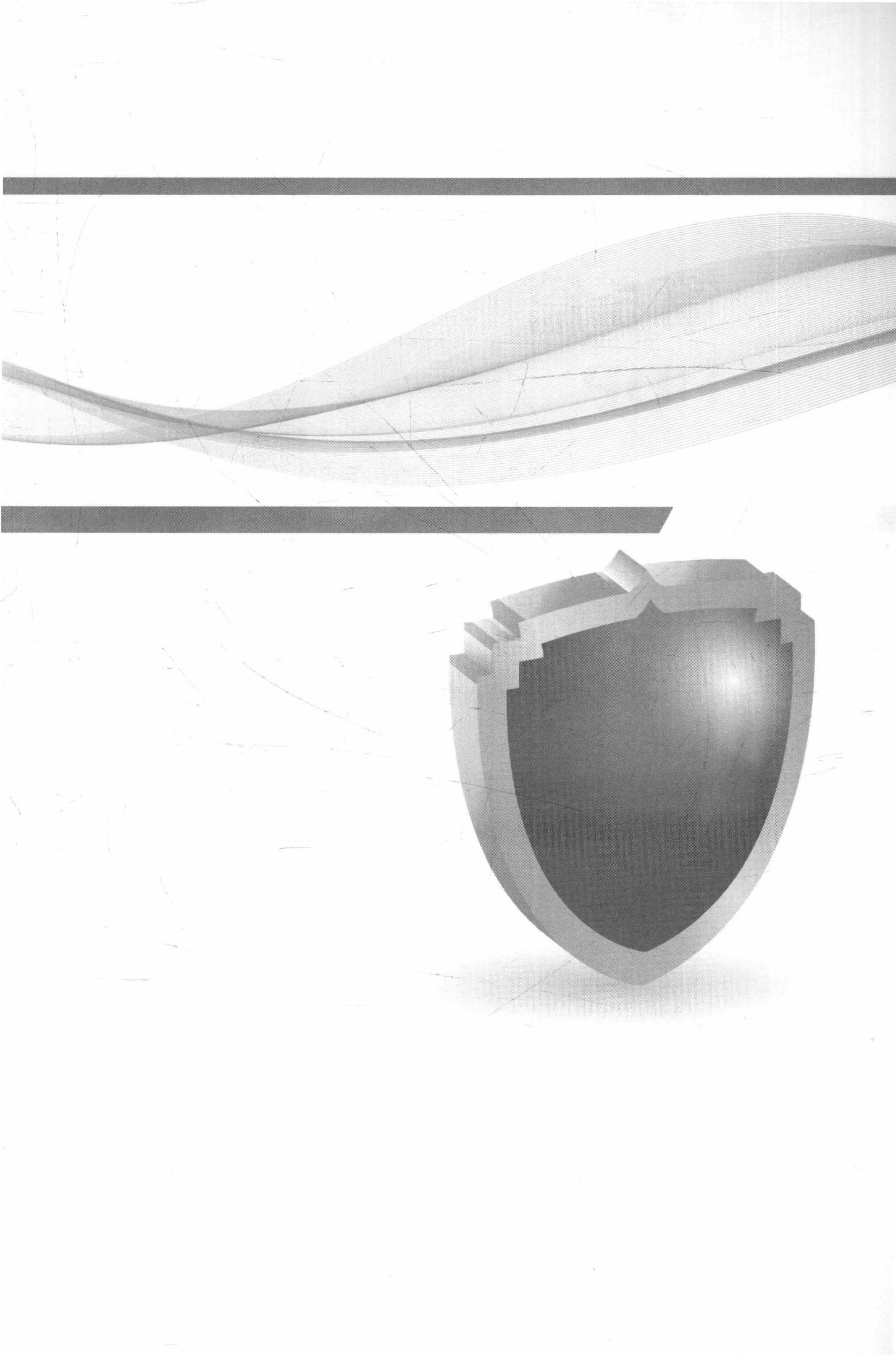


图 4-25 TCP 标志位异常

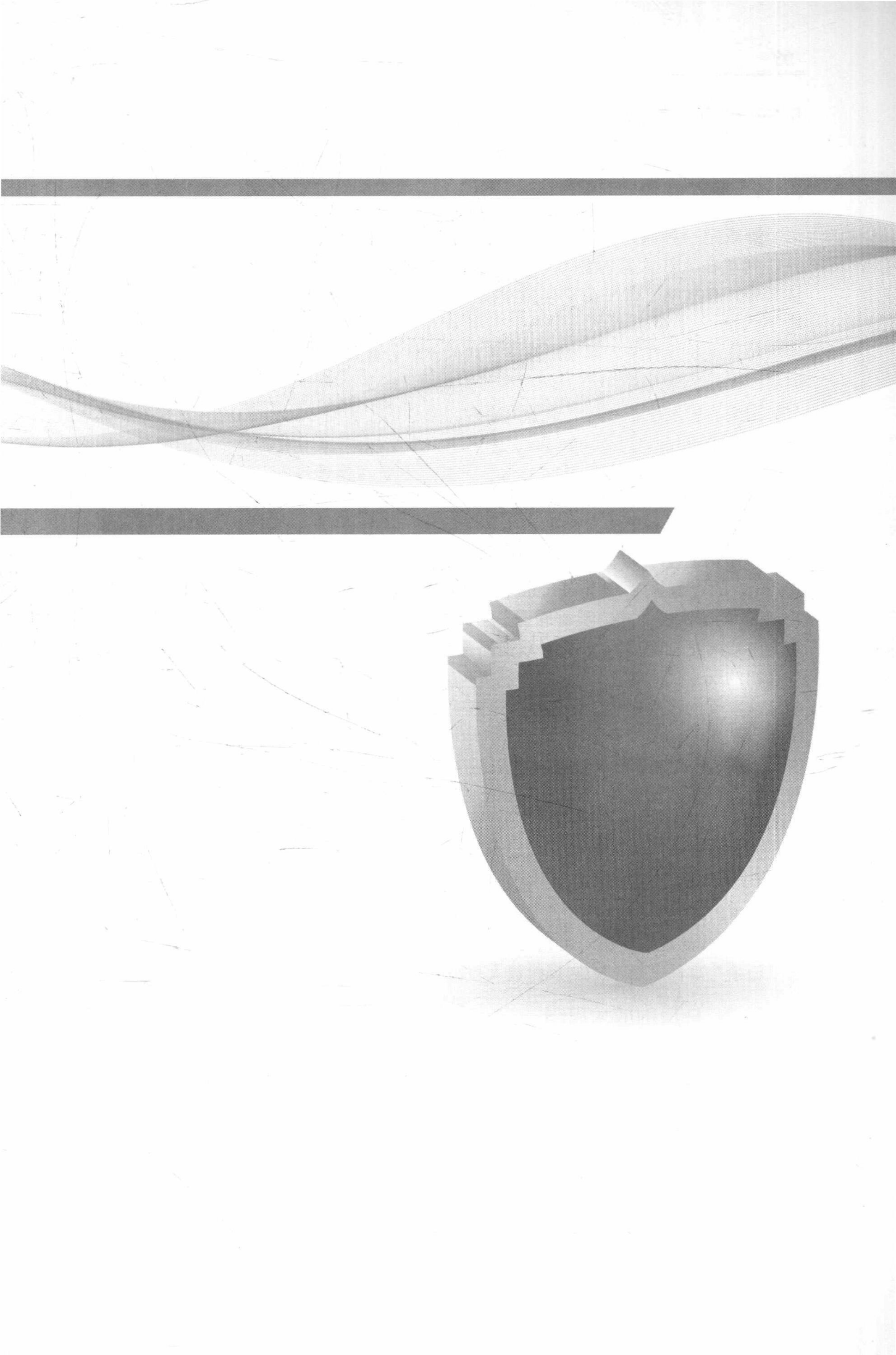
表 4-1 给出了 Anti-DDoS 系统判定 TCP 异常报文的原则，通过这些检查项，Anti-DDoS 系统可以全面准确地防御 TCP 异常报文攻击。

表 4-1 **TCP 异常标志位检查项**

六个标志位全为 1	六个标志位全为 0
SYN 标志位和 FIN 标志位同时为 1	SYN 标志位和 RST 标志位同时为 1
FIN 标志位和 RST 标志位同时为 1	PSH 标志位、FIN 标志位和 URG 标志位同时为 1
仅 FIN 标志位为 1	仅 URG 标志位为 1
仅 PSH 标志位为 1	带有载荷的 SYN 报文和 SYN-ACK 报文
SYN 标志位、RST 标志位和 FIN 标志位为 1 的分片报文	



第5篇 UDP



5.1 热点事件解密之："网游大战"攻击事件

5.1.1 事件回顾

游戏是一种娱乐方式，网络游戏则是如今最红火的一个门类。从早期的魔兽世界，到现在大红大紫的英雄联盟，网络游戏的不断发展，融入了更多对抗性元素。这其中，有战略、有平衡、有操作技巧。网络游戏比赛也就有了一个高大上的名字，电子竞技。

对许多游戏开发者而言，网络游戏的诞生使命是，"通过互联网服务中的网络游戏服务，提升全球人类生活品质"。本节的案例，即是和网游有关。

网游界曾发生了一起"追杀"事件。事件的主角是 PhantmL0rd（玩家）和黑客组织 DERP Trolling。PhantomL0rd，本名 James Varga，某专业游戏小组的成员，同时是美国最大的在线游戏直播平台 Twitch 的知名和资深视频博主，经常一边参加游戏对战一边实况直播。DERP Trolling，一个成立于 2011 年的黑客组织，本次事件中专门以"PhantomL0rd"实况直播的游戏为攻击目标，一旦成功击倒目标，便会在推特上发布战果。事情看上去很简单。这一天，PhantmL0rd 连续在多场游戏对战中遭到 DERP Trolling 的"追杀"：凡是 PhantmL0rd 参加的网络游戏，都不同程度地遭到了 DERP Trolling 的 DDoS 攻击。英雄联盟、EA 官网、暴雪战网、DOTA2 官网、企鹅俱乐部等知名游戏网站都因遭到 DDoS 攻击而瘫痪。然而，随着事件的不断被挖掘和曝光，知道真相的玩家们震惊了。调查发现，一直被认为是受害者的 PhantomL0rd 实际上恰恰是这次事件的幕后主使。这是什么原因呢？原来，PhantomL0rd 经常参加一些游戏对战比赛，既然是比赛就会有胜有负。但是 PhantomL0rd 为了保住自己"王"的地位，就偷偷地和 DERP Trolling 串通：一旦比赛过程中 PhantomL0rd 打不过对手，DERP Trolling 就登场，向游戏服务器发动 DDoS 攻击，让比赛异常终止，这样 PhantomL0rd 就有翻盘的机会。

这次事件的曝光不仅让 PhantomL0rd 颜面尽失，还让 DERP Trolling 使用的这个 DDoS 攻击手段"火"了一把。那么 DERP Trolling 到底使用了什么手段呢？

DERP Trolling 在这次"追杀"事件中，采用的是 NTP 反射放大攻击。从记载来看，DERP Trolling 应该是第一个利用 NTP 服务器进行大规模反射放大攻击的黑客组织。这次"追杀"事件之后，NTP 反射放大攻击一夜之间变得非常火热。

5.1.2 NTP 反射放大攻击

NTP（Network Time Protocol，网络时间协议），它是用来保证网络中的计算机时间同步的协议。在网络中，计算机的时间同步非常的重要。

如图 5-1 所示，NTP 采用服务器——客户端模型，它提供了高精准度的时间校正机制。在网络中，NTP 客户端不以自己的时间为准，而是每隔一段时间从 NTP 服务器同步更新自身的时间。NTP 定义了 NTP 服务器的层次结构，通过逐层传播，实现时间同步。上游 NTP 服务器通常是高精度且可靠的时钟源，如原子钟、卫星、天文台等，时间同步的精度得到了保证。

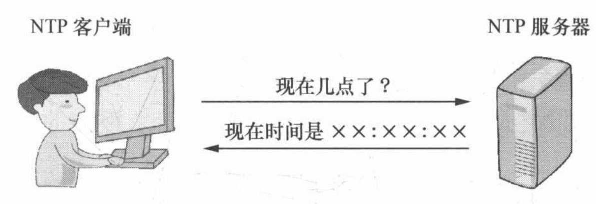


图 5-1 NTP 模型

NTP 中有一个监控（Monlist）功能，该功能用于监控 NTP 服务器。NTP 服务器会记录与自己进行过时间同步的客户端 IP 地址的信息，而且客户端可以通过一些命令索要这些记录。每个 NTP 服务器可以记录进行过时间同步的最后 600 个客户端的 IP 地址，当有客户端索要这个记录时，如图 5-2 所示，NTP 服务器会返回这 600 个客户端 IP 地址。响应包按照每 6 个 IP 地址进行分割，最多可以返回 100 个响应包。

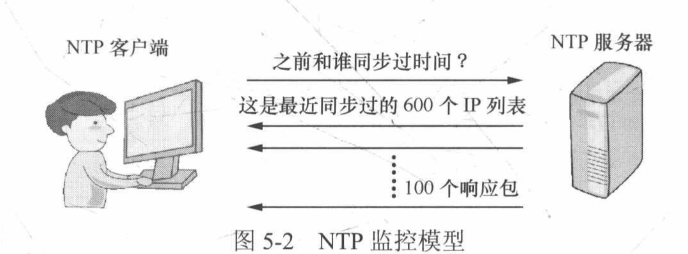


图 5-2 NTP 监控模型

理解了 NTP，NTP 反射放大攻击就容易理解了。NTP 反射放大攻击有两个关键点：反射和放大。

1. 反射

反射就是把源 IP 地址伪造成被攻击 IP 地址，进行“传瞎话”的行为。缺少源认证机制的协议最容易被利用，反射攻击均为基于 UDP 的无状态连接协议。NTP 正是基于 UDP 进行传输的。

UDP 中，正常情况下，客户端发送请求包到服务器，服务器返回响应包给客户端，这就完成了一次交互，中间没有校验过程。由于 UDP 是面向无连接的 NTP 服务器，客户端发送的请求包的源 IP 地址很容易被篡改。版本较低的 NTP 服务器没有针对源 IP 地址的校验机制，如果把请求包的源 IP 地址篡改为攻击目标的 IP 地址，最终服务器返回的响应包就会被送到攻击目标的 NTP 服务器中，这就是“反射”攻击，如图 5-3 所示。

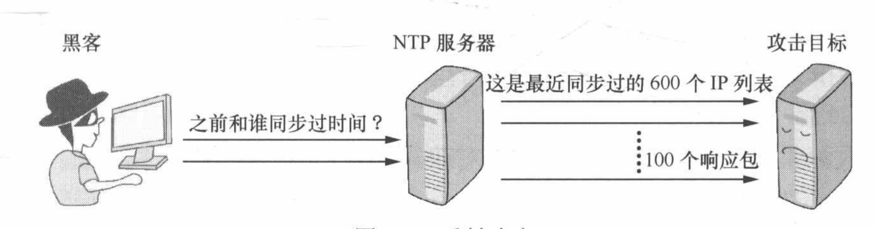


图 5-3 反射攻击

2. 放大

放大，顾名思义，就是我假冒你的名义打他一拳，他会打你 100 拳。黑客通常是利用互联网的基础架构来进行放大攻击。在网络中，开放的 NTP 服务器非常多，如果

黑客利用僵尸主机，同时向 NTP 服务器发起大量的 Monlist 请求，1 个 Monlist 请求包可以引发 100 个响应包。通常，1 个 NTP 请求包有 90 字节的大小，而 1 个回应报文为 482 字节，100 个回应报文是 48200 字节，回应报文是请求报文的 500 倍左右，如图 5-4 所示。

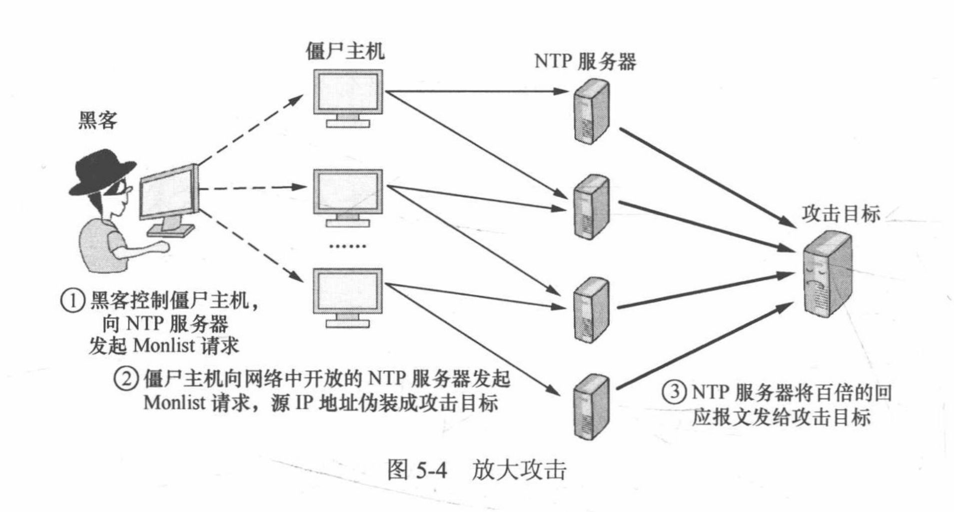


图 5-4　放大攻击

5.1.3 华为 Anti-DDoS 系统的解决方案

我们了解了 NTP 反射放大攻击原理，其他的 UDP 反射放大攻击也就都容易理解了。那么，防御 UDP 反射攻击的有效方式就是围绕以下两点进行。

（1）无状态防御；

（2）大流量防御。

华为 Anti-DDoS 系统具有一套完整、灵活的过滤机制和强大的设备处理能力，可以较好地解决 UDP 反射放大攻击。

1. 特征过滤

我们应对 UDP 反射放大攻击最有效、最直接的防御手段就是特征过滤。其根据攻击报文的特征，自定义过滤条件。

UDP 反射放大攻击有两个特点：一是属于 UDP，二是目的端口号固定。我们在防御 UDP 反射放大攻击时，从这两个特征入手，将已知的攻击特征，直接配置到过滤器的参数中。在配置静态指纹过滤后，Anti-DDoS 会对收到的报文进行特征匹配，对匹配到攻击特征的报文，再进行丢弃、限流等下一步操作，如图 5-5 所示。

2. 高性能

这种大流量的反射放大攻击的防御对防御系统的性能要求也非常高。Anti-DDoS 系统硬件 AntiDDoS8000 是一款分布式 Anti-DDoS 设备，其容量大、可靠性高、可扩展性强。

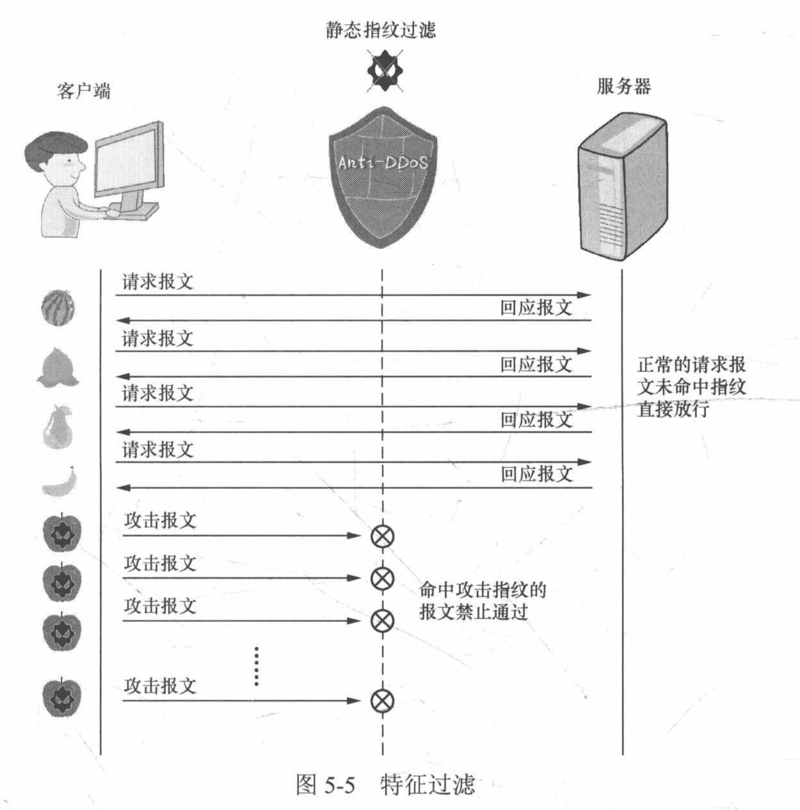


图 5-5　特征过滤

① Anti-DDoS 设备单槽位防御性能最大支持 160G bit/s/60M bit/s，整机扩容能力强，其中 AntiDDoS8160 可以最大支持 1.44TB 容量。

② Anti-DDoS 设备所有关键的组件都是 1:1 备份，转发和控制分离。

③ 系统扩容只需要直接插入接口板或者业务板，接口板会自动分流到各业务板；业务板所有 CPU 互为备份，负载均衡。

5.2　UDP 解析

UDP（User Datagram Protocol，用户数据报协议）是一种传输层协议，一种无连接的协议。它不提供数据包的分组、组装，不对数据包的传输进行确认，当报文被发送出去后，发送端不关心报文是否能够完整的到达对端。这个看似是缺点，但是 UDP 最大的优点。这种报文处理方式决定了 UDP 资源消耗小、处理速度快，因此音频、视频和普通数据传送时通常使用 UDP。

相比于前文介绍的 DNS 和 HTTP，UDP 需要关注的点要简单很多。下面，我们来了解 UDP 报文格式，如图 5-6 所示。

我们再来看一个现网真实 UDP 报文的抓包，如图 5-7 所示。

每个 UDP 报文由 UDP 报文头部和 UDP 数据字段两部分组成。头部字段由 8 个字节，4 个字段组成，分别是：源端口号、目的端口号、报文长度和校验和。

① UDP 使用端口号为不同的应用保留其各自的数据传输通道。比如 DNS 协议目的

端口号是 53；TFTP 目的端口号是 69。

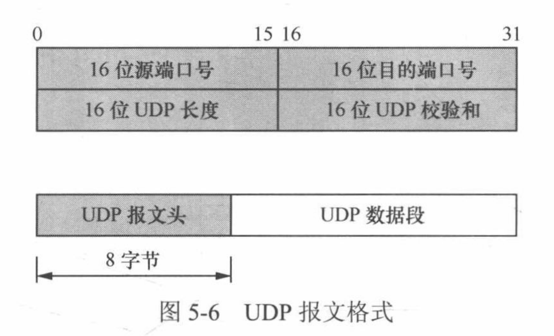


图 5-6 UDP 报文格式

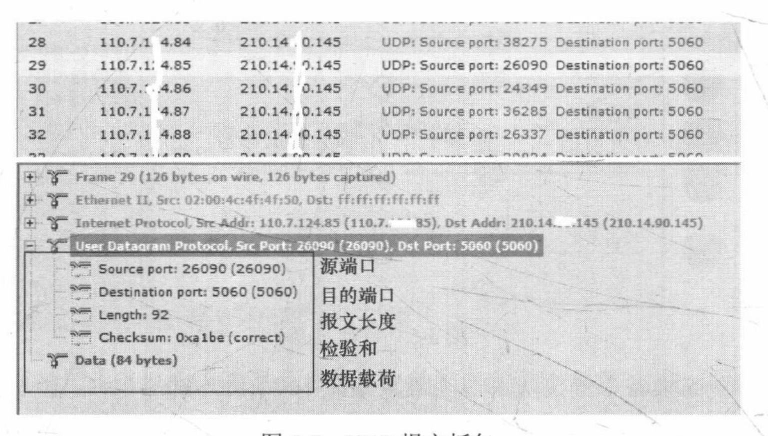


图 5-7 UDP 报文抓包

② 数据报的长度是指包括报头和数据载荷部分在内的总字节数。因为报头的长度是固定的，所以该域主要被用来计算可变长度的数据载荷部分。数据载荷的最大长度根据操作环境的不同而各异。从理论上说，包含报头在内的数据报文的最大长度为 65535 字节。不过，一些实际应用往往会限制报文的大小。

③ UDP 使用报头中的校验值来保证数据的安全。校验值首先在数据发送方通过特殊的算法计算得出，在传递到接收方之后，还需要再重新计算。如果某个数据报在传输过程中被第三方人为篡改或者因其他原因遭到了损坏，发送和接收方的校验计算值将不会相符，UDP 可以检测报文传输过程中是否出错。虽然 UDP 提供错误检测，但检测到错误时，UDP 不做错误校正，只是简单地把损坏的报文丢弃，或者给应用程序提供警告信息。

5.3 UDP Flood 攻击与防御

5.3.1 UDP Flood 攻击原理

UDP Flood 攻击原理很简单，通常是黑客控制僵尸主机，向目标服务器发送大量的

UDP 报文，通过消耗网络带宽等方式，达到攻击效果，如图 5-8 所示。UDP Flood 攻击一般具有如下几种方式。

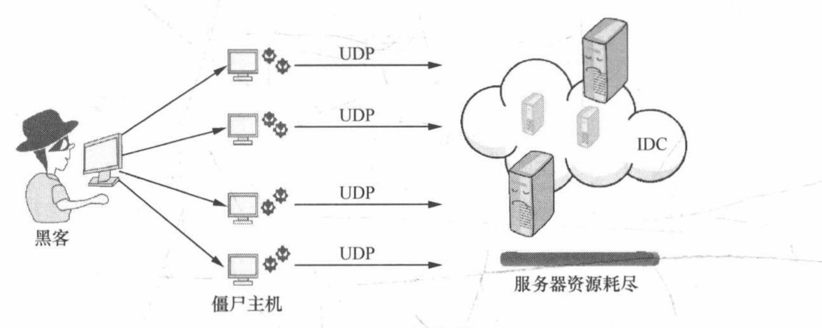


图 5-8　UDP Flood 攻击原理

① 黑客发送的 UDP 报文很大，而且速率非常快，消耗网络带宽资源，严重时造成链路拥塞。

② 大量源变端口的 UDP Flood 会导致依靠会话转发的网络设备，性能降低甚至会话耗尽，从而导致网络瘫痪。

③ 黑客攻击某个 UDP 业务端口，服务器检查报文的正确性时会消耗计算资源，影响服务器的正常业务。

5.3.2　华为 Anti-DDoS 系统如何防御 UDP Flood 攻击

UDP 与 TCP 不同，UDP 是一种无连接的协议，并且 UDP 应用五花八门，差异极大，因此针对 UDP Flood 的防护非常困难。我们也不能像 TCP 攻击那样进行源认证，所以只能找特征了。

传统的 UDP 攻击都是由攻击工具打出来的，通常会具有一定的特征，尤其在数据段会有一些相同或者有规律变化的字段。5.2 节介绍的 UDP 反射放大攻击，虽然并不是攻击工具伪造的 UDP 报文，但是由真实网络设备发出的 UDP 报文。数据段不具备相同的特征，但是目的端口却是固定的，也可以作为一种特征。

在确定攻击报文的特征后，我们要根据特征进行过滤。特征过滤也就是我们常说的指纹过滤。

指纹过滤有以下两种方法。

1. 静态指纹过滤

对于已知的攻击特征，可以直接配置到过滤器的参数中。Anti-DDoS 系统不仅具有 TCP、UDP 等的报文解析能力，还具有应用层报文解析能力。它可针对应用层头部信息字段做过滤。配置了静态指纹过滤后，Anti-DDoS 会对收到的报文进行特征匹配，对匹配到攻击特征的报文，再进行丢弃、限流等下一步操作，如图 5-9 所示。

我们通过抓包分析获知攻击特征。人为识别出攻击特征，然后配置到过滤器中。UDP 报文的数据段、源 IP 地址、源端口，目的 IP 地址、目的端口都可能隐藏着攻击报文。

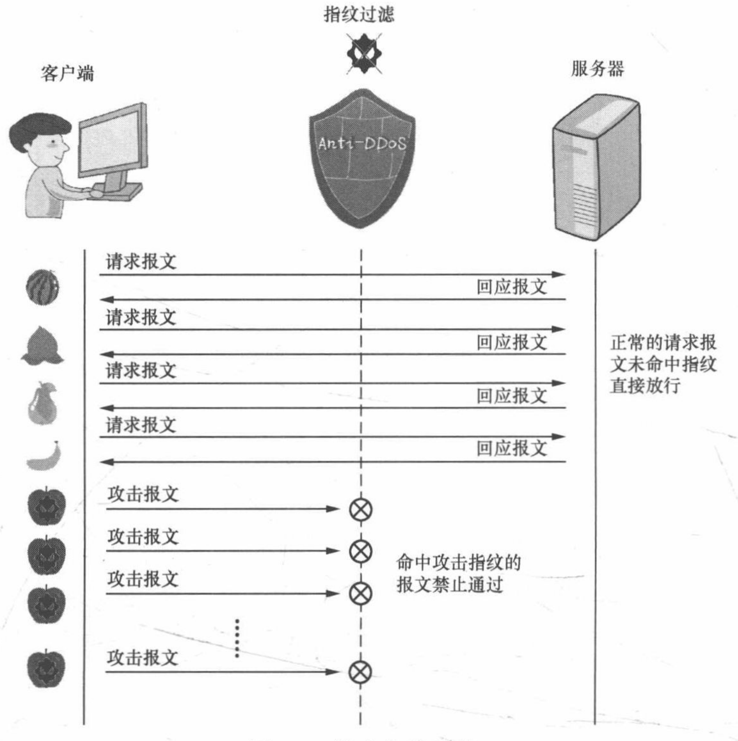


图 5-9 静态指纹过滤

此外，Anti-DDoS 系统还提供了 14 种常见 UDP 反射放大攻击的过滤器模板，见表 5-1。这些攻击都属于已知攻击特征，Anti-DDoS 系统已经预先定义好了攻击特征的参数，只需要直接应用即可。

表 5-1 过滤器模板

NTP 反射放大攻击	DNS 反射放大攻击
SNMP 反射放大攻击	SSDP 反射放大攻击
Chargen 反射放大攻击	QOTD 反射放大攻击
TFTP 反射放大攻击	Quake 反射放大攻击
NetBIOS 反射放大攻击	Wordpress 反射放大攻击
Steam 反射放大攻击	SQL 反射放大攻击
Portmapper 反射放大攻击	RIPV1 反射放大攻击

2. 动态指纹学习

在攻击特征未知的情况下，Anti-DDoS 系统具有指纹自动学习的功能。对于一些攻击工具发起的 UDP 攻击，攻击报文都拥有相同的特征字段。指纹学习就是对一些有规律的 UDP 攻击报文负载特征进行识别，并且自动提取出指纹特征，然后把这个提取的特征作为过滤条件，自动应用并进行过滤，如图 5-10 所示。

当然，这个学习的偏移量和学习长度都是可以手动配置的。偏移量是从 UDP 报文头结束处开始计算，取值从 0 字节到 1500 字节可灵活配置；学习长度从 1 个字节开始配置，最多可以学习 8 个字节。

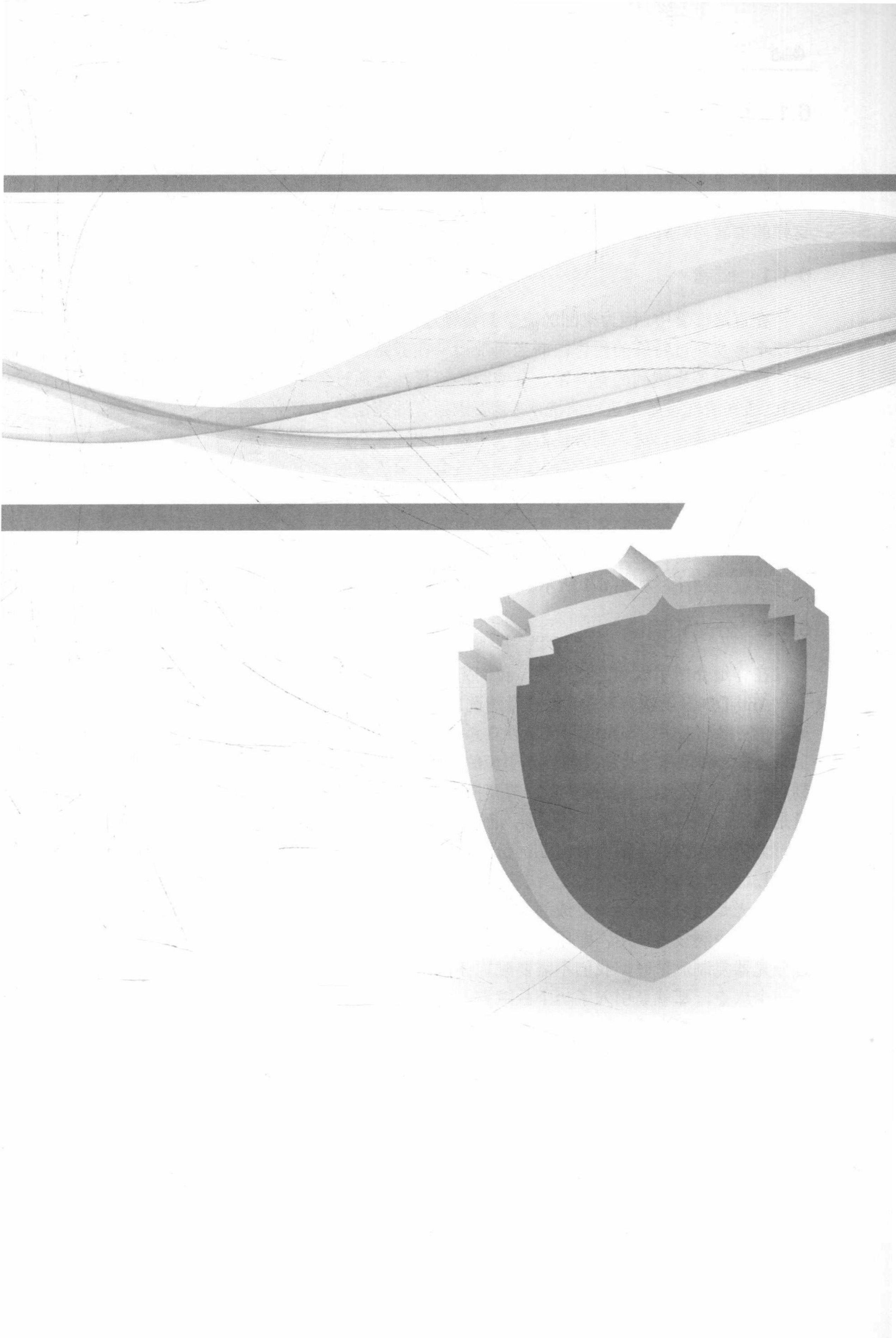


图 5-10　动态指纹学习

传统的 UDP Flood 攻击是一种消耗对方资源，也消耗自己资源的攻击方式，黑客攻击了一个服务器，其实也在消耗自己的系统资源。

近几年 UDP 反射放大攻击常被黑客所使用。后续对 UDP Flood 攻击的防御重点也应该聚焦在反射放大攻击上。

第 6 篇 配 置



6.1 引流

华为 Anti-DDoS 解决方案的部署模式分为直路部署、旁路静态引流部署和旁路动态引流部署 3 种方式。除直路部署外，其他两种方式中的清洗设备都处于旁挂位置，对于这样的部署，异常的流量要完成清洗并到达最终目的地还需要经过引流和回注两个过程。

6.1.1 概念

在直路部署中，因为来回的流量都会经过设备转发，所以不需要经过特殊的操作；而当清洗设备在旁路部署时，检测设备检测到的有异常、有威胁的流量，会通过 ATIC 通知清洗设备来进行清洗，这就要求原有的流量要改变当前的路径，进入到旁挂的清洗设备上来，这个过程我们称为引流。引流完成后，清洗设备会对引进来的流量进行清洗，即把异常、有威胁的流量剔除，留下正常的业务流量。清洗完成后，需要再把流量返回到原有的路径上，最终发送到目的地。这个返回流量到原路径的过程就是回注，如图 6-1 所示。

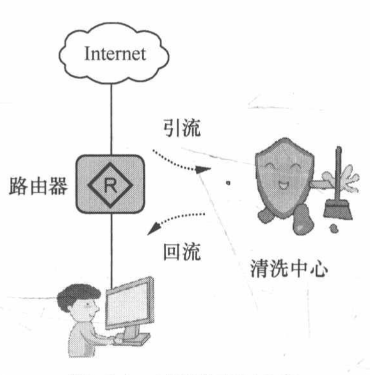


图 6-1　引流回注示意

6.1.2 分光和镜像

在详细介绍引流和回注之前，我们先来了解下分光和镜像的概念。

Anti-DDoS 解决方案中，在流量清洗之前，我们都知道还有一个很重要的环节——检测，在网络部署中，如果检测设备独立旁路部署，也需要将网络中的流量引导到检测设备上来。分光和镜像就是为检测设备引流的手段，不过我们引入的不是真实的流量，而是复制后的流量。这是因为检测设备只需要检测出流量中是否含有威胁即可，至于检测出的流量是真实的还是复制的是无所谓的，而且使用复制的流量不会影响正常业务的转发。

分光和镜像都是将流量复制一份到检测设备，但处理方式又不相同。

1. 分光

分光是通过分光器来完成的，它是一个独立的硬件，数据通过分光器后会将数据复制一份供检测设备使用，即原来的流量正常通行，同时分一股出来供检测设备分析。通过分光器复制流量时，我们不需要配置任何命令，只要有输入光即可。但是，这也带来了一个缺点，那就是引入了一个故障点，同时也正是因为它是一个在线设备，所以在部署时，需要中断当前网络，这对业务会产生一定的影响。

2. 镜像

镜像分为端口镜像和流镜像。端口镜像是指将流经被监控端口的某个方向（入、出、双向）的所有报文复制到指定的目标端口进行分析。流镜像是在端口镜像的基础上增加了流分类条件，只复制满足特定条件的报文，过滤不关心的报文，从而提高报文分析设备的工作效率。对于 Anti-DDoS 检测设备来说，我们要分析所有进入网络的流量是否存在异常，所以我们一般都是通过端口镜像功能来复制流量的，如图 6-2 所示。在端口镜像中：

① 被监控的端口称为镜像端口。

② 指定的目标端口称为观察端口。

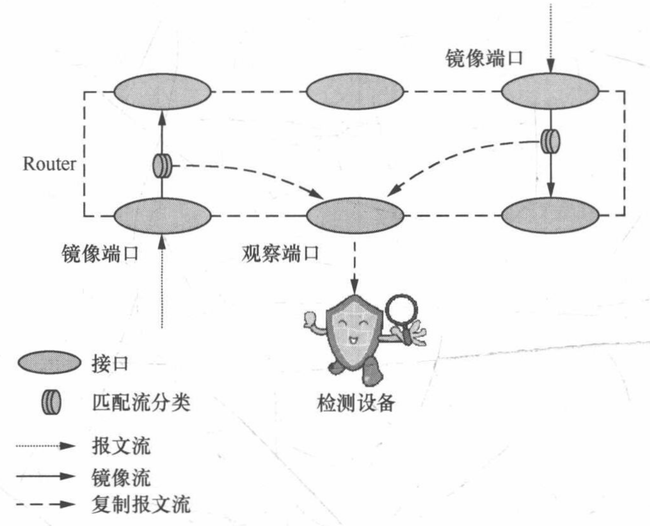


图 6-2　端口镜像示意

如图 6-3 所示的组网中，我们需要在 Router1 上和检测设备上配置相关命令，具体配置参考见表 6-1。这里 Router1 以华为 NE80E 路由器为例，检测设备以华为 Anti DDoS8000 系列为例进行介绍。

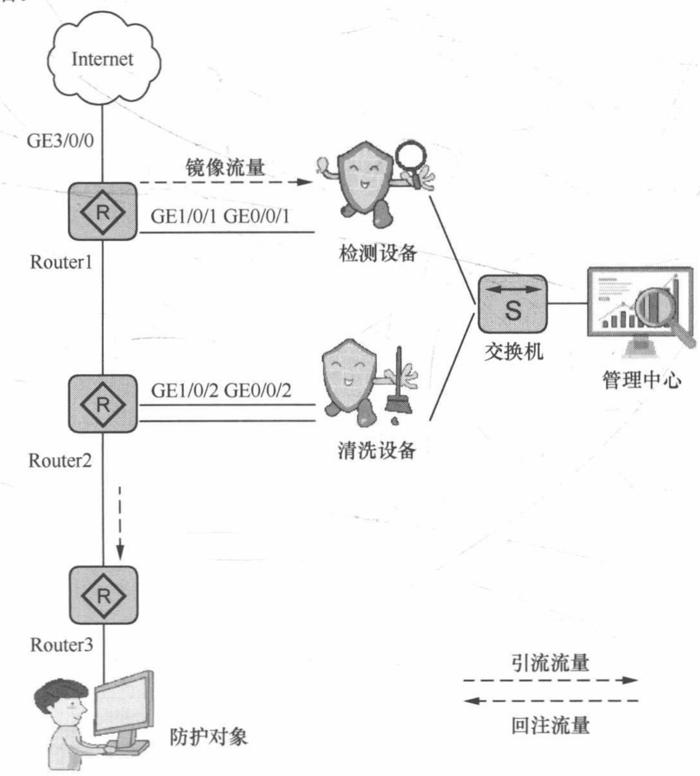


图 6-3　端口镜像组网示意

表 6-1 端口镜像配置表

NE80E 路由器	AntiDDoS8000 系列
1. 配置 GE1/0/1 为观测端口 <Router1> system-view [Router1] interface gigabitethernet1/0/1 [Router1-GigabitEthernet1/0/1] port-observing observe-index 1 [Router1-GigabitEthernet1/0/1] quit 2. 配置整板镜像的观测端口 [Router1] slot 3 [Router1-slot-3] mirror to observe-index 1 [Router1-slot-3] quit 3. 在 GE3/0/0 上使能上行端口镜像功能 [Router1] interface gigabitethernet3/0/0 [Router1-GigabitEthernet3/0/0] port-mirroring inbound	1. 指定业务板子卡的检测功能 <AntiDDoS8000> system-view [AntiDDoS8000] firewall ddos detect-spu slot 1 card 1 2. 配置检测设备的接口功能 [AntiDDoS8000] interface gigabitethernet0/0/1 [AntiDDoS8000-GigabitEthernet0/0/1] anti-ddos detect enable [AntiDDoS8000-GigabitEthernet0/0/1] anti-ddos flow-statistic enable

配置中，Router1 上配置观测端口的索引号必须与该接口所在的接口板的槽位号一致。在 slot 3 上配置令 mirror to observe-index 1 命令后，此观测索引对应的观测端口将作为整个 3 接口板的观测端口，当此接口板上有接口进行镜像时，报文就会被镜像到这个整板镜像的观测端口上。

完成上述配置后，端口 GE3/0/0 上接收的所有报文将被镜像到端口 GE1/0/0 上发往 AntiDDoS8000 系列检测设备。AntiDDoS8000 系列检测设备需设置相应的检测板，以及在接口配置检测功能和开启流量统计功能。完成这些配置后，就可以对接收的流量进行分析检测了。

对比分光和镜像，它们各有优劣，具体对比见表 6-2。

表 6-2 分光和镜像对比表

对比项	分光	镜像
适用场景	需要部署分光器，成本较高，常用于运营商网络	需要在网络设备上增加观测端口，不需要额外部署其他设备或器件。成本低，常用于企业网络
部署难度	需要安装分光器，安装简单	需要在分流的网络设备上配置镜像功能，有一定难度
对用户网络的影响	透明接入不影响原有网络拓扑，但分光会导致原来网络的光信号的光功率下降，会影响光信号的传输距离	不影响原有的网络拓扑
对用户业务的影响	安装分光器时需要短暂中断业务	配置镜像时不影响正常业务的转发

在网络部署中，请根据网络实际情况进行合理选择。

华为 Anti-DDoS 解决方案支持多种类型的检测设备，其中，AntiDDoS8000 系列、AntiDDoS1600 系列检测设备是采用逐包检测的方法对流量进行检测，即对流量中的所

有报文进行检测，所以通过分光和镜像功能将流量全部复制到检测设备上来。还有一些其他的检测设备，如华为 NFA2000V、威睿 GenieATM 等，这类检测设备是逐流检测方式，它们的检测流量来源是通过各种流采集分析协议来完成的，比如 Cisco 的 Netflow 协议、华为的 NetStream 协议等。这类流采集分析协议是对网络中不同的流进行提取，然后分类统计，最后将统计信息输出给检测设备进行分析检测，而不是像分光和镜像那样直接复制流量。

6.1.3 引流方法

分光、镜像是复制流量输出给检测设备进行检测；流采集分析协议是提取流量特征，将符合条件的流统计信息给检测设备进行分析，这些措施都不会影响实际的业务流量转发。然而对于清洗设备来说，我们需要清洗的是实际业务流量中的威胁或异常内容，如果清洗设备旁挂，我们必须要改变原有的业务转发路径，把流量引导到清洗设备上来，而通过分光和镜像等显然是不能完成的。那当清洗设备旁路部署时，为实现流量清洗，我们需要如何进行引流呢？

华为 Anti-DDoS 解决方案支持的引流可分为静态引流和动态引流两种。

① 静态引流：手动创建并下发引流策略到清洗设备引发引流，业务流量无论是否发生异常，都将改变原有流量的路径将流量引流到清洗设备。

② 动态引流：检测设备发现异常通告管理中心，管理中心自动生成引流策略并下发到清洗设备；攻击结束，管理中心向清洗设备下发取消引流策略。

如果按照具体的配置方法来划分，可分为策略路由引流和 BGP 引流。

① 策略路由引流：在引流的网络设备上配置策略路由，将目的地址为防护对象的流量发送到清洗设备。

② BGP 引流：通过在引流的网络设备和清洗设备上配置 BGP 实现引流。

策略路由引流通常用于静态引流方式，BGP 引流根据配置的不同可以是静态引流方式，也可以是动态引流方式。

下面我们先从策略路由引流的具体实现和配置说起。

1. 策略路由引流

策略路由（Policy-based Routing）也称为路由重定向（Redirect），顾名思义是指基于策略的路由机制。通常，路由设备是根据报文目的地址查找路由表进行报文转发的，而策略路由是一种依据用户制定的策略进行路由选择的机制，策略路由的操作对象是数据包，在路由表已经产生的情况下，不按照先行路由表进行转发，而是根据需要，依照某种策略改变其转发路径的方法。

策略路由引流，正是根据这种策略，改变报文原有的转发路径，引导流量到清洗设备上来。

在图 6-4 中，Router1 为引流设备，为了对到达防护对象的流量进行清洗，可以在 Router1 的 GE1/0/0 接口配置策略路由，让从外网通过 GE1/0/0 接口到达防护对象的流量改变原有路径从 GE1/0/1 接口转发到清洗设备进行清洗。

策略路由引流只需要在引流路由器 Router1 的 GE1/0/0 上配置策略路由，无需在清洗设备上进行任何配置。Router1 以华为 NE80E 路由器为例，具体配置如下。

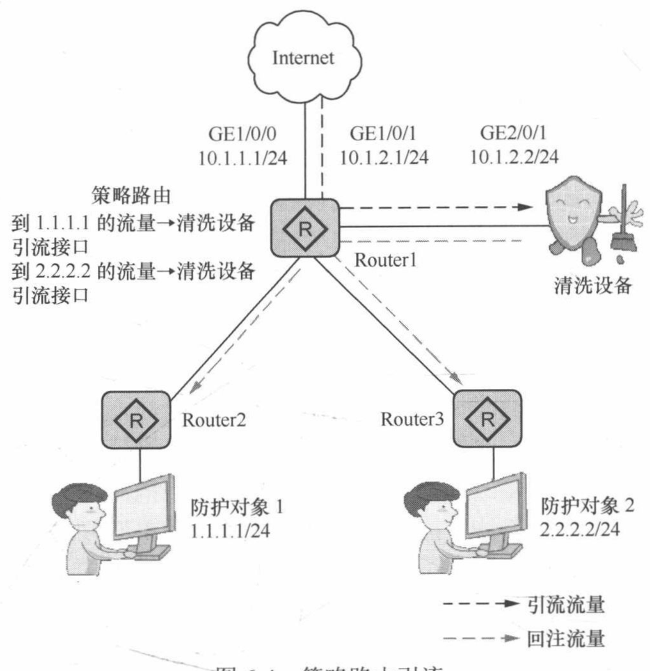


图 6-4 策略路由引流

（1）定义流分类

```
[Router1] acl 3001
[Router1-acl-adv-3001] rule permit ip destination 1.1.1.1 0
[Router1-acl-adv-3001] rule permit ip destination 2.2.2.2 0
[Router1-acl-adv-3001] quit
[Router1] traffic classifier class1
[Router1-classifier-class1] if-match acl 3001
[Router1-classifier-class1] quit
```

（2）配置流行为并配置报文转发动作

```
[Router1] traffic behavior behavior1
[Router1-behavior-behavior1] redirect ip-nexthop 10.1.2.2 interface
GigabitEthernet 1/0/1
[Router1-behavior-behavior1] quit
```

（3）定义流量策略并在策略中为类指定行为

```
[Router1] traffic policy policy1
[Router1-trafficpolicy-policy1] classifier class1 behavior behavior1
[Router1-trafficpolicy-policy1] quit
```

（4）在接口上应用策略路由

```
[Router1] interface GigabitEthernet 1/0/0
[Router1-GigabitEthernet1/0/0] traffic-policy policy1 inbound
[Router1-GigabitEthernet1/0/0] quit
```

策略路由引流，配置比较简单，操作方便，但使用这种引流方式时，如果回注流量的链路 Down 了，业务流量还是会通过策略路由被送到清洗设备上来，这样清洗后的流量又不能回注回去，势必造成业务的中断。所以，为了保证引流策略路由也能及时 Down 掉，我们可以在清洗设备上配置类似 Link-group 的功能，将引流和回注链路加入到一个 Link-group 中，形成联动，回注的链路 Down 了，引流的链路也及时 Down 掉，从而保证业务的正常转发。

除此之外，策略路由引流不考虑流量中是否存在异常，统一地将流分类中定义的所

有流量都送到清洗设备进行处理。正常的流量也会转发到清洗设备上来，一方面影响了正常业务的转发效率；另一方面也会消耗清洗设备的部分资源，造成不必要的浪费。相比之下，BGP 引流会更加高效智能。

2. BGP 引流

BGP 是一种用于自治系统（Autonomous System，AS）之间的动态路由协议，它的引流其实是需要 Anti-DDoS 解决方案中多个设备配合完成的。

BGP 引流分为静态引流和动态引流两种（其中动态引流又分为自动和手动），它们的区别在于：静态引流，无论检测设备是否检测到异常，管理中心都会生成针对防护对象 IP 地址/IP 地址段的引流任务，这种引流任务需要由管理员手工创建；而动态引流是当检测设备检测到异常时，管理中心会自动生成引流任务，引流任务生成后系统会将其直接下发（自动）或者通过管理员手动下发（手动）到清洗设备。异常或攻击结束后，系统会自动取消引流。

不管是 BGP 的静态引流还是动态引流，管理中心都会下发一条引流任务到清洗设备，此时，清洗设备上会为每个防护对象自动生成一条 32 位主机 UNR（User Network Route，用户网络路由），此路由的下一跳为与清洗设备回注接口直连的路由设备的接口地址，即下图中 Router1 的 GE1/0/2 接口地址。

生成路由后，清洗设备会将这条 UNR 路由引入 BGP 中，并通过 BGP 发布给 BGP 邻居 Router1，此时，Router1 上就会有一条目的地址为防护对象、下一跳为清洗设备的引流接口的 32 位主机路由。

后续，Router1 收到 Internet 发来的到防护对象的报文时，查找路由表，根据最长掩码匹配原则，优先匹配这条路由，从而转发到清洗设备上来进行流量清洗，如图 6-5 所示。

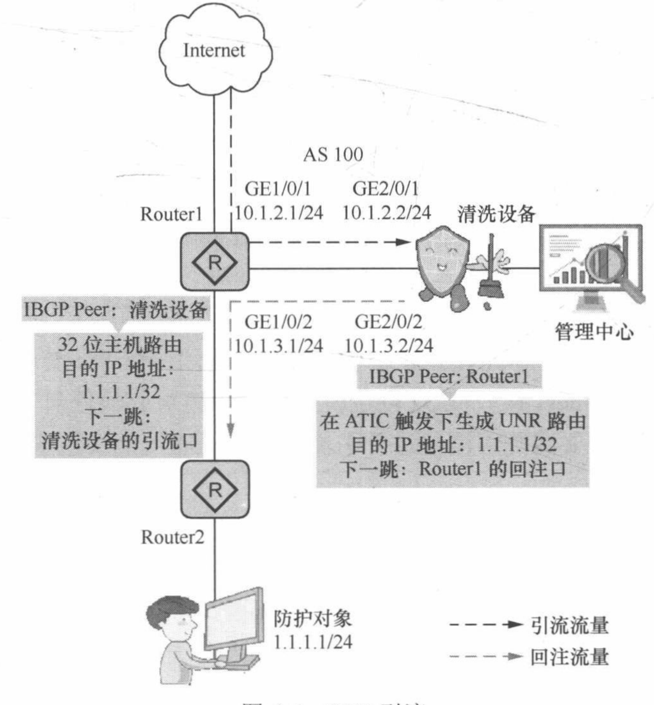


图 6-5 BGP 引流

BGP 引流需要在 Router1、清洗设备和管理中心上配置，引流部分的具体配置步骤如下。

首先，在管理中心界面上选择“防御>策略配置>引流”，创建引流任务，配置被保护的 IP 地址为 1.1.1.1，子网掩码为 255.255.255.255，单击“确定”。

然后在清洗设备上，设置 32 位主机 UNR 路由下一跳地址，这里的下一跳为 Router1 回注接口 GE1/0/2 的 IP 地址。

```
[sysname]   firewall ddos bgp-next-hop 10.1.3.1
```

上述步骤配置完成后，清洗设备上会生成一条到达 1.1.1.1 的 32 位主机 UNR 路由，下一跳为 10.1.3.1。

```
[sysname] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
      Destinations : 8          Routes : 8

Destination/Mask     Proto   Pre   Cost        Flags NextHop         Interface
     1.1.1.1/32   Direct    0      0            D    10.1.3.1   GigabitEthernet2/0/2
---- More ----
```

关于 BGP 部分的配置见表 6-3，其中 Router1 以华为 NE80E 路由器为例。

表 6-3 BGP 引流关键配置

NE80E	清洗设备
[Router1] bgp 100 [Router1-bgp] peer 10.1.2.2 as-number 100 [Router1-bgp] quit	[sysname] route-policy 1 permit node 1 [sysname-route-policy] apply community no-advertise [sysname-route-policy] quit [sysname] bgp 100 [sysname-bgp] peer 10.1.2.1 as-number 100 [sysname-bgp] import-route unr [sysname-bgp] ipv4-family unicast [sysname-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export [sysname-bgp-af-ipv4] peer 10.1.2.1 advertise-community [sysname-bgp-af-ipv4] quit [sysname-bgp] quit

配置 apply community no-advertise 命令，用于设置团体属性，其在 BGP 路由策略中应用后，通告对等体 Router1 接收此 32 位主机路由后不再对其他任何对等体发布此路由，因为此路由只用于对需要清洗的流量进行引流，对外发布可能会造成不可预知的影响，如路由环路等。

相比策略路由引流，BGP 引流更加灵活，既能对防护对象进行静态引流，达到策略路由引流的效果，也能根据流量异常情况进行动态智能化引流，合理控制清洗设备的资源，方便管理员维护管理。

引流完成后，清洗设备会对异常流量进行清洗。清洗后的正常流量需要通过回注过程让业务流量能够回到原有网络中。

6.2 回注

6.2.1 常用回注方法

在华为 Anti-DDoS 解决方案中，能够将清洗后的流量回注到原网络中的配置方法有很多，常用的有如下几种。

① 二层回注：清洗设备通过二层方式将流量回注到防护对象，而不通过路由转发。

② 静态路由回注：通过在清洗设备上配置静态路由，引导清洗后的流量回到原网络中。

③ UNR 路由回注：与静态路由类似，通过在清洗设备上生成的 UNR 路由，将清洗后的流量回注到原网络，最后送到防护对象。

④ 策略路由回注：通过在清洗设备和路由器上配置策略路由，将清洗后的流量回注到不同的路径，最后送到防护对象。

⑤ GRE tunnel 回注：通过在清洗设备和回注路由器之间建立 GRE 隧道，将流量直接送到回注路由器上，最后送到防护对象。

⑥ MPLS LSP 回注：清洗设备和回注路由器之间建立 MPLS LSP，清洗后的流量在清洗设备上被打上单层标签，之后按预先建立好的 LSP 将其回注到原链路，最后送到防护对象。

⑦ MPLS VPN 回注：清洗设备和回注路由器之间建立 MPLS L3VPN，将清洗后的流量通过 MPLS L3VPN 回注到原链路，最后送到防护对象。

该如何选择回注方式呢？在 Anti-DDoS 解决方案中，引流和回注是配合使用的，我们推荐的引流回注方案见表 6-4。

表 6-4　引流回注方案对应表

流量引导方案	策略路由引流（静态引流）	BGP 引流（静态引流/动态引流）
二层回注	×	√
静态路由回注	√	√
UNR 路由回注	×	√
策略路由回注	√	√
GRE tunnel 回注	×	√
MPLS LSP 回注	×	√
MPLS VPN 回注	×	√

一方面我们可以根据引流策略来选择匹配的回注方式，另一方面我们也要考虑网络的实际部署情况适合何种回注策略。表 6-4 中我们已经有推荐的配套方案，接下来我们将详细介绍各种回注方式的特点、适用场景以及相关的配置。

1. *二层回注*

二层回注应用于清洗设备和防护对象之间都是二层网络的场景，在这种部署中，清洗设备上回注口的 IP 地址和防护对象的属于同一网段。完成流量清洗后，清洗设备通过

ARP 报文获得防护对象目的 IP 的 MAC 地址，而后将清洗后的正常流量发送到核心交换机，最终发送到防护对象。

在图 6-6 中，清洗设备旁路部署在核心三层交换机 Switch1 上，通过接口 GE2/0/1 与 Switch1 接口 GE1/0/1 直连。在清洗设备上配置子接口 GE2/0/1.10 和 GE2/0/1.20 分别关联 Switch1 上的 VLAN10 和 VLAN20 后，形成两个逻辑通道，一个用作引流，一个用作回注。

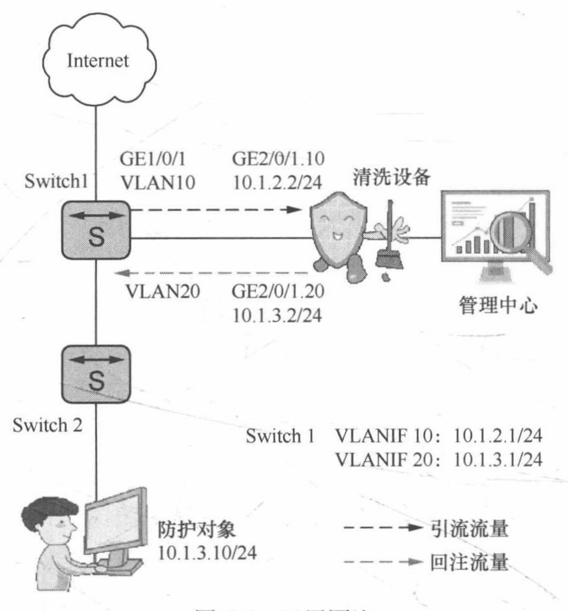


图 6-6 二层回注

对于引流，在前面的章节中有详细介绍，它可以通过配置 BGP 功能来完成。而清洗后的流量，配置二层回注后，清洗设备会发送 ARP Request 报文请求防护对象 IP 对应的 MAC 地址，收到防护对象的回应后，清洗设备将清洗后的流量根据获取的 MAC 地址等信息进行二层封装，然后经过二层交换机回注到防护对象。表 6-5 中列出了关于引流回注的具体配置，其中核心交换机以华为 S9300 系列为例。

表 6-5 二层回注关键配置表

S9300 系列	清洗设备
创建 VLAN <switch1> system-view [switch1] vlan 10 [switch1-vlan10] quit [switch1] vlan 20 [switch1-vlan20] quit 配置接口属性并关联 VLAN [switch1] interface gigabitethernet 1/0/1 [switch1-GigabitEthernet1/0/1] port link-type trunk [switch1-GigabitEthernet1/0/1] port trunk allow-pass vlan 10 20	# 配置子接口 GE2/0/1.10 的 IP 地址，并关联 VLAN10 <sysname> system-view [sysname] interface GigabitEthernet 2/0/1.10 [sysname-GigabitEthernet2/0/1.10] vlan-type dot1q 10 [sysname-GigabitEthernet2/0/1.10] ip address 10.1.2.2 24 [sysname-GigabitEthernet2/0/1.10] qui # 配置子接口 GE2/0/1.20 的 IP 地址，并关联 VLAN20 [sysname] interface GigabitEthernet 2/0/1.20 [sysname-GigabitEthernet2/0/1.20] vlan-type dot1q 20 [sysname-GigabitEthernet2/0/1.20] ip address 10.1.3.2 24 [sysname-GigabitEthernet2/0/1.20] quit

（续表）

S9300 系列	清洗设备
[switch1-GigabitEthernet1/0/1] quit [switch1] interface gigabitethernet 1/0/2 [switch1-GigabitEthernet1/0/2] port link-type trunk [switch1-GigabitEthernet1/0/2] port trunk allow-pass vlan 20 [switch1-GigabitEthernet1/0/2] quit 配置 VLANIF 接口的 IP 地址 [switch1] interface vlanif 10 [switch1-Vlanif10] ip address 10.1.2.1 24 [switch1-Vlanif10] quit [switch1] interface vlanif 20 [switch1-Vlanif20] ip address 10.1.3.1 24 [switch1-Vlanif20] quit 配置 BGP 功能 [switch1] bgp 100 [switch1-bgp] peer 10.1.2.2 as-number 100 [switch1-bgp] quit	# 配置生成动态路由时使用的下一跳地址 [sysname] firewall ddos bgp-next-hop 10.1.2.1 # 对生成的 32 位主机 UNR 路由进行 FIB 过滤 [sysname] firewall ddos bgp-next-hop fib-filter # 配置 BGP 功能及团体属性 [sysname] route-policy 1 permit node 1 [sysname-route-policy] apply community no-advertise [sysname-route-policy] quit [sysname] bgp 100 [sysname-bgp] peer 10.1.2.1 as-number 100 [sysname-bgp] import-route unr [sysname-bgp] ipv4-family unicast [sysname-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export [sysname-bgp-af-ipv4] peer 10.1.2.1 advertise-community [sysname-bgp-af-ipv4] quit [sysname-bgp] quit # 在清洗口开启流量统计功能 [sysname] interface GigabitEthernet 2/0/1.10 [sysname-GigabitEthernet2/0/1.10] anti-ddos flow-statistic enable [sysname-GigabitEthernet2/0/1.10] quit

在上述配置中，BGP 的配置用于引流，引流的配置还需要在管理中心上进行相应设置。二层回注的配置比较简单，只需要在核心交换机 Switch1 上让与清洗设备回注接口互联的接口和连接防护对象的接口加入同一 VLAN 即可，保证二层连接互通。当然核心交换机到防护对象之间要求没有三层设备。相对于其他回注方法而言，二层回注是唯一的一个不需要通过路由回注清洗后流量的回注方法。

2. UNR 路由回注

UNR 一般是通过非本设备配置的路由，与 IGP、BGP、静态路由、直连路由等路由一样，可以添加到路由表中指导报文转发。我们知道，在 BGP 引流中，管理员通过 ATIC 创建引流任务，配置被保护的防护对象地址，同时在清洗设备上配置下一跳 IP 地址，就会在清洗设备上生成一条目的地址为防护对象的 UNR。此 UNR 被清洗设备上 BGP 引入后发布给引流设备，从而对需要清洗的流量进行引流，这就是 UNR 在引流中的作用，如图 6-7 所示。

除此之外，这条 UNR 也可以对清洗后的流量进行回注。如图 6-7 组网中，清洗设备和 ATIC 完成配置后，清洗设备上会生成一条到达 1.1.1.1 的 32 位主机 UNR，下一跳为 Router1 的回注接口 GE1/0/2 的 IP 地址 10.1.3.1。完成流量清洗后，根据路由查找的最长掩码匹配原则，优先选择此 UNR，将清洗后的流量回注到 Router1，此为 UNR 在流量回注中的应用。

大家可能会想到，在 BGP 引流的时候，Router1 从清洗设备 BGP 发布的路由中学习

到这条 32 位主机路由，访问防护对象的流量被此路由送到了清洗设备。现在，清洗设备又将这条流送到了 Router1，此时，Router1 上还会匹配这条主机路由将回注回来的流量再送到清洗设备，如此循环往复，就成了环路。所以，为了将清洗后的流量最终送到防护对象，我们还需要在 Router1 上配置策略路由，让从回注接口 GE1/0/2 进来的流量都从 GE1/0/3 进行转发。

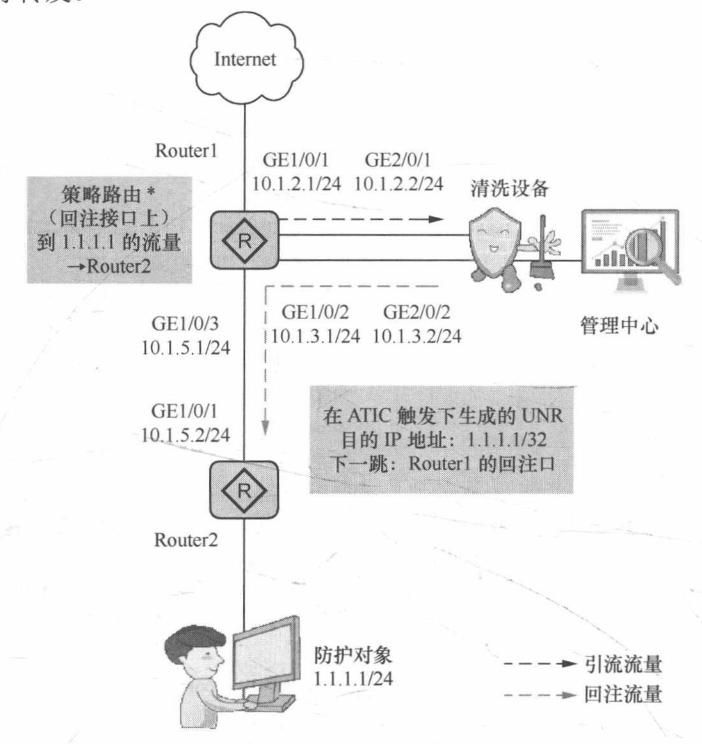


图 6-7 UNR 回注

关于引流回注的具体配置见表 6-6，其中 Router1 以华为 NE80E 路由器为例。

表 6-6 UNR 路由回注关键配置

Router1	清洗设备
配置 BGP 功能 [Router1] bgp 100 [Router1-bgp] peer 10.1.2.2 as-number 100 [Router1-bgp] quit 在接口 GE1/0/2 配置策略路由 # 定义流分类 [Router1] acl 3001 [Router1-acl-adv-3001] rule permit ip [Router1-acl-adv-3001] quit [Router1] traffic classifier class1 [Router1-classifier-class1] if-match acl 3001 [Router1-classifier-class1] quit # 配置流行为并配置报文转发动作 [Router1] traffic behavior behavior1	# 配置生成动态路由时使用的下一跳地址 <sysname> system-view [sysname] firewall ddos bgp-next-hop 10.1.3.1 # 配置 BGP 功能及团体属性 [sysname] route-policy 1 permit node 1 [sysname-route-policy] apply community no-advertise [sysname-route-policy] quit [sysname] bgp 100 [sysname-bgp] peer 10.1.2.1 as-number 100 [sysname-bgp] import-route unr [sysname-bgp] ipv4-family unicast [sysname-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export [sysname-bgp-af-ipv4] peer 10.1.2.1 advertise-community

（续表）

Router1	清洗设备
[Router1-behavior-behavior1] redirect ip-nexthop 10.1.5.2 interface GigabitEthernet 1/0/3	
[Router1-behavior-behavior1] quit	
# 定义流量策略并在策略中为类指定行为	[sysname-bgp-af-ipv4] quit
[Router1] traffic policy policy1	[sysname-bgp] quit
[Router1-trafficpolicy-policy1] classifier class1 behavior behavior1	# 在清洗口开启流量统计功能
	[sysname] interface GigabitEthernet 2/0/1
[Router1-trafficpolicy-policy1] quit	[sysname-GigabitEthernet2/0/1] anti-ddos flow-statistic enable
# 在接口上应用策略路由	
[Router1] interface GigabitEthernet 1/0/2	[sysname-GigabitEthernet2/0/1] quit
[Router1-GigabitEthernet1/0/2] traffic-policy policy1 inbound	
[Router1-GigabitEthernet1/0/2] quit	

除了上面的配置外，还需要在管理中心界面上选择“防御>策略配置>引流”，创建引流任务，配置被保护的IP地址为1.1.1.1，子网掩码为255.255.255.255，单击“确定”。如此才能在清洗设备上生成UNR。

整个配置比较简单，策略路由和BGP引流的配置在前面都有详细介绍，这里我们不再细分解。而回注的配置就是生成这条UNR的配置，以及回注路由器上的策略路由配置。

在实际应用中，回注路由器可以与引流路由器是同一个，也可以不是同一个，如可以是Router1，也可以是其他下行路由器（如Router2）。

3. 静态路由回注

静态路由回注与UNR回注使用场景和配置基本相同，不同之处有以下几点。

① 既然是静态路由回注肯定会配置静态路由，事实上这条静态路由与UNR除了协议类型不同，其他基本一样，目的地址都是防护对象，下一跳也都为回注路由器上的回注接口地址。两个路由产生的区别在于静态路由是在清洗设备上手动配置的，而UNR是在管理中心和清洗设备上进行相应设置后自动生成的，且掩码固定为32位。

② 静态路由回注还需要在清洗设备上配置一条firewall ddos bgp-next-hop fib-filter命令，表示过滤清洗设备生成的UNR，使清洗设备上的报文不能根据其进行转发。这是因为UNR掩码是32位，在路由查找中根据掩码最长匹配原则，报文首先匹配的是这条UNR，为了不影响流量通过其他回注策略转发，就需要在清洗设备上配置此命令过滤生成的这条UNR，使其不下发到FIB表中。除二层回注和UNR回注外，其他所有的回注策略都需要配置此命令。

除以上两点外，静态路由回注能与两种引流方法配合使用，而UNR回注只能与BGP引流成匹配方案。

静态路由回注如果与BGP引流配合，它的配置除增加回注的静态路由和过滤UNR的命令外，其他配置与UNR回注完全相同；静态路由与策略路由引流配合使用时，回注的配置只需按要求配置静态路由即可。因为配置比较简单，我们不再详细列出具体的配置。

以上 3 种回注方法虽然配置简单，但适用场景也相对有限，网络拓扑不能太复杂，比如二层回注要求回注网络固定为二层；UNR 回注只适用于单回注链路的场景，并且与 BGP 引流配合使用时，还要在引流设备上通过一定的方法避免路由环路的隐患，增加了引流设备上的配置难度，显然只有这些回注方法是不能满足各种网络情况下的流量回注需求的。为此，我们引入了策略路由和 GRE 两种回注方法，在一定程度上能解决相关问题，比如策略路由回注能应用在多回注链路的场景中；GRE 回注能直接避开引流路由，将回注流量直接送到下行学习不到引流路由的路由器上，避免了路由环路的问题。

4. 策略路由回注

在讲解引流的章节中，我们介绍过策略路由，策略路由是依照某种策略改变报文转发路径的方法，很显然通过策略路由这种改变报文转发路径的策略，我们也能将清洗后的流量回注到原来的路径上去。

策略路由回注可以与 BGP 引流和策略路由引流配合使用，但部署配置上有所区别。

在图 6-8 中，Router1 为引流路由器，引流流量从 GE1/0/1 接口进入清洗设备，完成流量清洗后，在清洗设备上通过配置策略路由可以让访问不同防护对象的流量进入不同的回注通道返回到原有网络中。

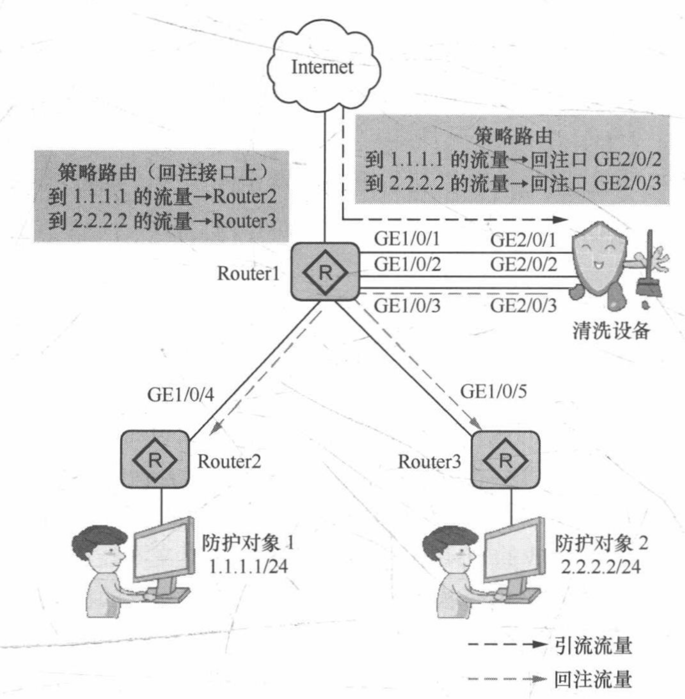


图 6-8 策略路由回注

（1）清洗设备

流量清洗后通过策略路由回注到 Router1 时，Router1 会根据路由表转发还会将流量送回清洗设备，从而形成路由环路。所以，还需要在 Router1 的回注入接口上配置策略路由，将回注流量送到下行 Router2 或 Router3，继续转发。路由回注过程如下。

① 在清洗设备的引流入接口 GE2/0/1 上应用策略路由，将不同防护对象的流量回注到 Router1 不同的接口 GE1/0/2 和 GE1/0/3。

② 在 Router1 回注入接口 GE1/0/2 和 GE1/0/3 上分别应用策略路由，将流量送给下行 Router2 或 Router3，最后将流量送到防护对象。

（2）策略路由

Router1 和清洗设备之间不存在路由环路的问题，只需要在清洗设备上应用策略路由，就可以实现回注的过程，具体过程如下。

① 在清洗设备的引流入接口 GE2/0/1 上应用策略路由，将不同防护对象的流量回注到 Router1 不同的接口。

② 回注流量到达 Router1 后，通过查找路由表，将流量送到下行 Router2 或 Router3，最后将流量送到防护对象。

下面我们以 BGP 引流与策略路由回注为例，讲解具体的配置，其中各接口地址规划见表 6-7。

表 6-7　接口地址规划

设备名称	接口	IP 地址
清洗设备	GE2/0/1	10.1.2.2/24
	GE2/0/2	10.1.3.2/24
	GE2/0/3	10.1.4.2/24
Router1	GE1/0/1	10.1.2.1/24
	GE1/0/2	10.1.3.1/24
	GE1/0/3	10.1.4.1/24
	GE1/0/4	10.1.5.1/24
	GE1/0/5	10.1.6.1/24
Router2	GE1/0/1	10.1.5.2/24
Router3	GE1/0/1	10.1.6.2/24

配置见表 6-8。

表 6-8　策略路由回注关键配置

Router1	清洗设备
配置 BGP 功能 [Router1] bgp 100 [Router1-bgp] peer 10.1.2.2 as-number 100 [Router1-bgp] quit 在接口 GE1/0/2 配置策略路由 # 定义流分类 [Router1] acl 3001 [Router1-acl-adv-3001] rule permit ip source 1.1.1.0 0.0.0.255 [Router1-acl-adv-3001] quit [Router1] traffic classifier class1 [Router1-classifier-class1] if-match acl 3001 [Router1-classifier-class1] quit # 配置流行为并配置报文转发动作 [Router1] traffic behavior behavior1 [Router1-behavior-behavior1] redirect ip-nexthop 10.1.5.2 interface GigabitEthernet 1/0/4	# 配置生成动态路由时使用的下一跳地址 <sysname> system-view [sysname] firewall ddos bgp-next-hop 10.1.3.1 # 对生成的 32 位主机 UNR 进行 FIB 过滤 [sysname] firewall ddos bgp-next-hop fib-filter # 配置 BGP 功能及团体属性 [sysname] route-policy 1 permit node 1 [sysname-route-policy] apply community no-advertise [sysname-route-policy] quit [sysname] bgp 100 [sysname-bgp] peer 10.1.2.1 as-number 100 [sysname-bgp] import-route unr [sysname-bgp] ipv4-family unicast [sysname-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export [sysname-bgp-af-ipv4] peer 10.1.2.1 advertise-community [sysname-bgp-af-ipv4] quit

（续表）

Router1	清洗设备
[Router1-behavior-behavior1] quit # 定义流量策略并在策略中为类指定行为 [Router1] traffic policy policy1 [Router1-trafficpolicy-policy1] classifier class1 behavior behavior1 [Router1-trafficpolicy-policy1] quit # 在 GE1/0/2 接口上应用策略路由 [Router1] interface GigabitEthernet 1/0/2 [Router1-GigabitEthernet1/0/2] traffic-policy policy1 inbound [Router1-GigabitEthernet1/0/2] quit 在接口 GE1/0/3 配置策略路由 # 定义流分类 [Router1] acl 3002 [Router1-acl-adv-3002] rule permit ip source 2.2.2.0 0.0.0.255 [Router1-acl-adv-3002] quit [Router1] traffic classifier class2 [Router1-classifier-class2] if-match acl 3002 [Router1-classifier-class2] quit # 配置流行为并配置报文转发动作 [Router1] traffic behavior behavior2 [Router1-behavior-behavior2] redirect ip-nexthop 10.1.6.2 interface GigabitEthernet 1/0/5 [Router1-behavior-behavior2] quit # 定义流量策略并在策略中为类指定行为 [Router1] traffic policy policy2 [Router1-trafficpolicy-policy2] classifier class2 behavior behavior2 [Router1-trafficpolicy-policy1] quit # 在 GE1/0/3 接口上应用策略路由 [Router1] interface GigabitEthernet 1/0/3 [Router1-GigabitEthernet1/0/3] traffic-policy policy2 inbound [Router1-GigabitEthernet1/0/2] quit	[sysname-bgp] quit # 在清洗口开启流量统计功能 [sysname] interface GigabitEthernet 2/0/1 [sysname-GigabitEthernet2/0/1] anti-ddos flow-statistic enable [sysname-GigabitEthernet2/0/1] quit # 在清洗设备接口 GE2/0/1 配置策略路由，实现回注功能，让访问不同防护对象的流量从不同接口转发 [sysname] policy-based-route [sysname-policy-pbr] rule name huizhu1 [sysname-policy-pbr-rule-huizhu1] ingress-interface GigabitEthernet 2/0/1 [sysname-policy-pbr-rule-huizhu1] destination-address 1.1.1.1 24 [sysname-policy-pbr-rule-huizhu1] action pbr egress-interface GigabitEthernet 2/0/2 next-hop 10.1.3.1 [sysname-policy-pbr-rule-huizhu1] quit [sysname-policy-pbr] rule name huizhu2 [sysname-policy-pbr-rule-huizhu2] ingress-interface GigabitEthernet 2/0/1 [sysname-policy-pbr-rule-huizhu2] destination-address 2.2.2.2 24 [sysname-policy-pbr-rule-huizhu2] action pbr egress-interface GigabitEthernet 2/0/3 next-hop 10.1.4.1 [sysname-policy-pbr-rule-huizhu2] quit [sysname-policy-pbr] quit

因为是 BGP 引流，因此还需要在管理中心界面上，选择“防御 > 策略配置 > 引流”，创建引流任务，配置被保护的 IP 地址为 1.1.1.1 和 2.2.2.2，子网掩码为 255.255.255.255，单击“确定”。如此才能在清洗设备上生成 UNR。

策略路由回注配置关键是要找准入口和出口，了解流量从哪进，从哪出，特别是当出现多个回注出口时，不要混淆。

策略路由回注是一种常用的回注方式，一般用于存在多个回注接口的情况。由于策略路由回注配置简单，通常推荐用户使用。

5. GRE 回注

GRE（General Routing Encapsulation，通用路由封装协议）是一种三层 VPN 封装技术。

GRE 的用途一般是对某些网络层协议（如 IPX、Apple Talk、IP 等）的报文进行封装，使封装后的报文能够在另一张网络中（如 IPv4）传输，从而解决跨越异种网络的报文传输问题。然而，在 GER 回注中使用 GRE 隧道是让报文跨越直连网络，能够传输到更远的网络。

在图 6-9 中，Router1 为引流路由器，引流流量通过 GE1/0/1 接口进入清洗设备，完成流量清洗后，回注的流量是通过 GRE 隧道直接传输到 Router2。

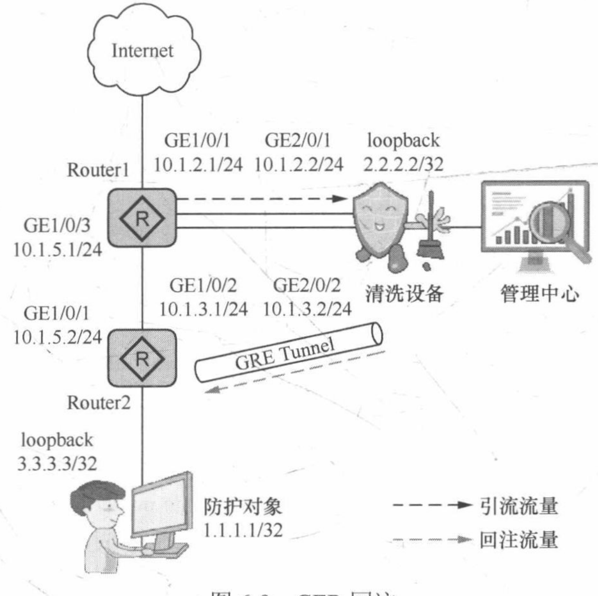


图 6-9　GER 回注

引流方式为 BGP 引流的场景，GRE 回注可以直接避开引流路由，将回注流量直接送到下行学习不到引流路由的路由器，避免了路由环路的问题。可能大家会问，不通过 GRE 隧道，我们也可以将回注链路通过物理连线直接连到 Router2，这样也能避开路由环路。是的，确实是这样，但是在 Router1 下面有很多路由设备的情况下，如果我们要创建多条回注链路，会给物理线路上的部署增加很多成本，而 GRE 隧道的逻辑连接却不存在这样的问题，只要保证清洗设备到各回注路由器之间路由可达即可。

GER 回注的配置见表 6-9，其中 Router1 和 Router2 以华为路由器 NE80E 为例。

表 6-9　**GER 回注关键配置表**

Router2	清洗设备
配置 Router2 的 loopback 地址 <Router2> set board-type slot 1 tunnel <Router2> system-view [Router2] interface loopback 1 [Router2-LoopBack1] ip address 3.3.3.3 32 [Router2-LoopBack1] target-board 1 [Router2-LoopBack1] binding tunnel gre [Router2-LoopBack1] quit 创建 Tunnel 接口，并指定源端接口和目的端接口 [Router2] interface Tunnel 1	在清洗设备上配置 GRE 功能 创建 Tunnel 接口，并指定源端接口和目的端接口。 <sysname> system-view [sysname] interface Tunnel 1 [sysname-Tunnel1] tunnel-protocol gre [sysname-Tunnel1] ip address 10.1.1.1 255.255.255.0 [sysname-Tunnel1] source 2.2.2.2 [sysname-Tunnel1] destination 3.3.3.3 [sysname-Tunnel1] quit 将 Tunnel 接口加入安全区域。Tunnel 接口加入的安全区域与源端接口 GE2/0/2 在同一个安全区域

（续表）

<table>
<tr><th>Router2</th><th>清洗设备</th></tr>
<tr><td>[Router2-Tunnel1] tunnel-protocol gre
[Router2-Tunnel1] ip address 10.1.1.2 255.255.255.0
[Router2-Tunnel1] source 3.3.3.3
[Router2-Tunnel1] destination 2.2.2.2
[Router2-Tunnel1] quit
配置 OSPF，通告各接口所连网段 IP 地址路由
[Router2] ospf 1
[Router2-ospf-1] area 0
[Router2-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255
[Router2-ospf-1-area-0.0.0.0] network 1.1.1.0 0.0.0.255
[Router2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[Router2-ospf-1-area-0.0.0.0] quit
[Router2-ospf-1] quit</td><td rowspan="3">[sysname] firewall zone trust
[sysname-zone-trust] add interface Tunnel 1
[sysname-zone-trust] quit
配置策略路由，将流量下一跳指向 Tunnel 接口
[sysname] policy-based-route
[sysname-policy-pbr] rule name gre1
[sysname-policy-pbr-rule-gre1] ingress-interface GigabitEthernet 2/0/1
[sysname-policy-pbr-rule-gre1] destination-address 1.1.1.1 32
[sysname-policy-pbr-rule-gre1] action pbr egress-interface Tunnel 1
[sysname-policy-pbr-rule-gre1] quit
[sysname-policy-pbr] quit
在清洗设备上，配置生成动态路由时使用的下一跳地址
[sysname] firewall ddos bgp-next-hop 10.1.3.1
对生成的 32 位主机 UNR 进行 FIB 过滤
[sysname] firewall ddos bgp-next-hop fib-filter
在清洗设备上配置 BGP 功能及团体属性
[sysname] route-policy 1 permit node 1
[sysname-route-policy] apply community no-advertise
[sysname-route-policy] quit
[sysname] bgp 100
[sysname-bgp] peer 10.1.2.1 as-number 100
[sysname-bgp] import-route unr
[sysname-bgp] ipv4-family unicast
[sysname-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export
[sysname-bgp-af-ipv4] peer 10.1.2.1 advertise-community
[sysname-bgp-af-ipv4] quit
[sysname-bgp] quit
在清洗设备的清洗口开启流量统计功能
[sysname] interface GigabitEthernet 2/0/1
[sysname-GigabitEthernet2/0/1] anti-ddos flow-statistic enable
[sysname-GigabitEthernet2/0/1] quit
配置清洗设备的 loopback 地址
[sysname] interface loopback 1
[sysname-LoopBack1] ip address 2.2.2.2 32
[sysname-LoopBack1] quit
配置 OSPF，通告各接口所连网段 IP 地址路由
[sysname] ospf 1
[sysname-ospf-1] area 0
[sysname-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[sysname-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[sysname-ospf-1-area-0.0.0.0] quit
[sysname-ospf-1] quit</td></tr>
<tr><th>Router1</th></tr>
<tr><td>配置 OSPF，通告各接口所连网段 IP 地址路由
[Router1] ospf 1
[Router1-ospf-1] area 0
[Router1-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[Router1-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255
[Router1-ospf-1-area-0.0.0.0] quit
[Router1-ospf-1] quit
配置 Router1 的 BGP 功能。
[Router1] bgp 100
[Router1-bgp] peer 10.1.2.2 as-number 100
[Router1-bgp] quit</td></tr>
</table>

除了上面的配置外，通过 BGP 引流都需要在管理中心上进行相关设置，具体的设置在前面的章节中都有详细介绍，本节中不再赘述。

从配置中我们看到，除引流、GRE 隧道以及 OSPF 动态路由协议配置外，清洗设备上还配置了策略路由，目的是让清洗后的流量从 Tunnel1 接口（GER 隧道）直接传送到 Router2，最终送到防护对象。所以，GRE 回注过程是通过策略路由配合 GRE 隧道来完成的。

GRE 回注虽然成功地避开了 BGP 引流路由，避免了路由环路的问题，但是在多回注通道场景中，依然需要管理员手动配置命令建立多个 GRE 隧道，如果网络拓扑发生变化，管理员还需要手动进行大量的配置调整，维护成本比较高。

策略路由回注也存在上述的问题，当网络变化较大，且防护对象 IP 地址很分散时，可能需要配置大量的策略路由。这时，一方面需要大量的人力维护；另一方面，清洗设备上配置过多策略路由也会影响系统性能。对此，我们推荐配置 MPLS 回注方式。MPLS 回注包含 MPLS LSP 回注和 MPLS VPN 回注两种方式。

6. MPLS LSP 回注

MPLS（Multiprotocol Label Switching，多协议标签交换技术）网络的基本组成单元是标签交换路由器（Label Switching Router，LSR），由 LSR 构成的网络区域称为 MPLS 域（MPLS Domain）。MPLS 基于标签进行转发。IP 包进入 MPLS 网络时，MPLS 入口的边缘路由器（Label Edge Router，LER）分析 IP 包的内容并且为这些 IP 包添加合适的标签，所有 MPLS 网络中的节点都是依据标签来转发数据的。当该 IP 包离开 MPLS 网络时，标签由出口 LER 删除。IP 包在 MPLS 网络中经过的路径称为标签交换路径（Label Switched Path，LSP）。LSP 是一个单向路径，与数据流的方向一致，如图 6-10 所示。

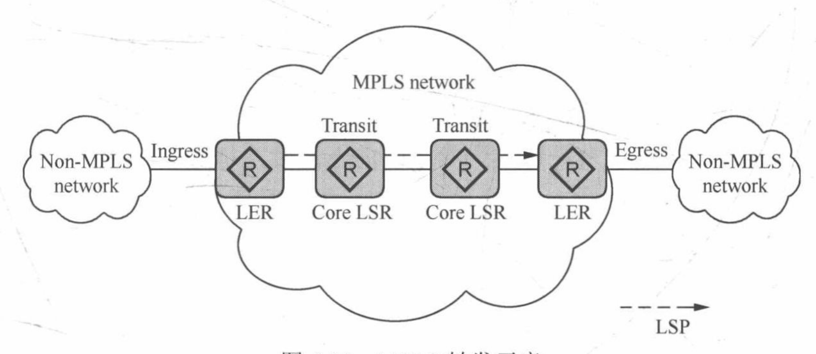


图 6-10　MPLS 转发示意

在回注策略中，MPLS LSP 回注就是让清洗后的流量通过这条 LSP 回注到原来路径。

在图 6-11 中，Router1 为引流路由器，访问防护对象的流量通过 BGP 引流到清洗设备进行清洗，清洗完成后，再通过 MPLS LSP 回注将清洗后的流量打上一层标签，按预先建立好的 LSP 回注到原链路。

LSP 的建立过程实际就是将转发等价类（Forwarding Equivalence Class，FEC）和标签进行绑定，并将这种绑定通告 LSP 上的相邻 LSR。FEC 是一组具有某些共性的数据流的集合。这些数据流在转发过程中被 LSR 以相同方式处理。在传统的采用最长匹配算法的 IP 转发中，到同一条路由的所有报文就是一个转发等价类，图 6-11 所示的防护对象 1.1.1.1/24、

2.2.2.2/24 就是不同的 EFC。

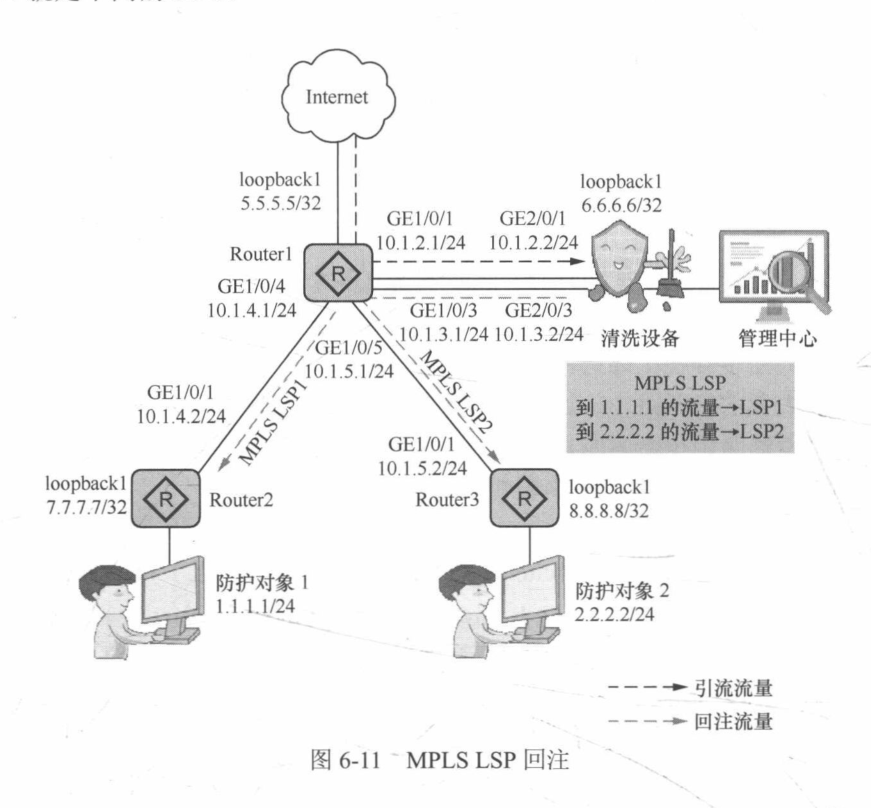


图 6-11 MPLS LSP 回注

在图 6-11 的组网中，LSP 建立过程如下。

MPLS 网络的边缘节点（图中的 Router2、Router3）发现自己的路由表中出现了新的主机路由（比如新加入防护对象），并且此路由的目的地址不属于任何现有的 FEC，则该边缘节点需要为这一目的地址建立一个新的 FEC。在边缘节点的路由设备上（Router2、Router3）为 FEC 分配标签，并主动向上游发出标签映射消息，标签映射消息中包含分配的标签和绑定的 FEC 等信息。收到标签映射消息的 LSR 在其标签转发表中增加相应的条目，然后主动向上游 LSR 发送指定 FEC 的标签映射消息。当入节点 LSR（清洗设备）收到标签映射消息时，它也需要在标签转发表中增加相应的条目。这时，就完成了 LSP 的建立，接下来就可以对该 FEC 对应的数据分组进行标签转发，即清洗后流量根据标签转发到最终防护对象。

按上述组网部署，MPLS LSP 回注的具体配置见表 6-10，其中 Router1、Router2、Router3 以华为 NE80E 为例。

表 6-10　　MPLS LSP 回注关键配置

Router1	清洗设备
配置 Router1 的 BGP 功能 [Router1] bgp 100 [Router1-bgp] peer 10.1.2.2 as-number 100 [Router1-bgp] quit 配置 Router1 的 loopback 地址	在清洗设备上，配置生成动态路由时使用的下一跳地址 <sysname> system-view [sysname] firewall ddos bgp-next-hop 10.1.3.1 对生成的 32 位主机 UNR 路由进行 FIB 过滤。

（续表）

Router1	清洗设备
[Router1] interface loopback 1 [Router1-LoopBack1] ip address 5.5.5.5 32 [Router1-LoopBack1] quit 配置 MPLS # 配置 MPLS 基本功能 [Router1] mpls lsr-id 5.5.5.5 [Router1] mpls [Router1-mpls] quit [Router1] mpls ldp [Router1-ldp] quit [Router1] interface GigabitEthernet 1/0/1 [Router1-GigabitEthernet1/0/1] mpls [Router1-GigabitEthernet1/0/1] mpls ldp [Router1-GigabitEthernet1/0/1] quit [Router1] interface GigabitEthernet 1/0/3 [Router1-GigabitEthernet1/0/3] mpls [Router1-GigabitEthernet1/0/3] mpls ldp [Router1-GigabitEthernet1/0/3] quit 配置 OSPF，通告各接口所连网段 IP 地址和 LSR ID 主机路由 [Router1] ospf 1 [Router1-ospf-1] area 0 [Router1-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255 [Router1-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255 [Router1-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0 [Router1-ospf-1-area-0.0.0.0] quit [Router1-ospf-1] quit	[sysname] firewall ddos bgp-next-hop fib-filter 在清洗设备上配置 BGP 功能及团体属性 [sysname] route-policy 1 permit node 1 [sysname-route-policy] apply community no-advertise [sysname-route-policy] quit [sysname] bgp 100 [sysname-bgp] peer 10.1.2.1 as-number 100 [sysname-bgp] import-route unr [sysname-bgp] ipv4-family unicast [sysname-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export [sysname-bgp-af-ipv4] peer 10.1.2.1 advertise-community [sysname-bgp-af-ipv4] quit [sysname-bgp] quit 在清洗设备的清洗口开启流量统计功能 [sysname] interface GigabitEthernet 2/0/1 [sysname-GigabitEthernet2/0/1] anti-ddos flow-statistic enable [sysname-GigabitEthernet2/0/1] quit 配置清洗设备的 loopback 地址 [sysname] interface loopback 1 [sysname-LoopBack1] ip address 6.6.6.6 32 [sysname-LoopBack1] quit 在清洗设备上配置 MPLS 功能，实现回注功能 # 配置 MPLS 基本功能 [sysname] mpls lsr-id 6.6.6.6 [sysname] mpls [sysname-mpls] quit [sysname] mpls ldp [sysname-ldp] quit [sysname] interface GigabitEthernet 2/0/3 [sysname-GigabitEthernet2/0/3] mpls [sysname-GigabitEthernet2/0/3] mpls ldp [sysname-GigabitEthernet2/0/3] quit # 配置 LSP 的触发建立策略 [sysname] mpls [sysname-mpls] lsp-trigger all [sysname-mpls] quit 配置 OSPF，通告各接口所连网段 IP 地址和 LSR ID 主机路由 [sysname] ospf 1 [sysname-ospf-1] area 0 [sysname-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255 [sysname-ospf-1-area-0.0.0.0] network 6.6.6.6 0.0.0.0 [sysname-ospf-1-area-0.0.0.0] quit [sysname-ospf-1] quit

（续表）

Router2	Router3
配置 Router1 的 loopback 地址	配置 Router1 的 loopback 地址
[Router2] interface loopback 1	[Router3] interface loopback 1
[Router2-LoopBack1] ip address 7.7.7.7 32	[Router3-LoopBack1] ip address 8.8.8.8 32
[Router2-LoopBack1] quit	[Router3-LoopBack1] quit
配置 MPLS	配置 MPLS
# 配置 MPLS 基本功能	# 配置 MPLS 基本功能
[Router2] mpls lsr-id 7.7.7.7	[Router3] mpls lsr-id 8.8.8.8
[Router2] mpls	[Router3] mpls
[Router2-mpls] quit	[Router3-mpls] quit
[Router2] mpls ldp	[Router3] mpls ldp
[Router2-ldp] quit	[Router3-ldp] quit
[Router2] interface GigabitEthernet 1/0/1	[Router3] interface GigabitEthernet 1/0/1
[Router2-GigabitEthernet1/0/1] mpls	[Router3-GigabitEthernet1/0/1] mpls
[Router2-GigabitEthernet1/0/1] mpls ldp	[Router3-GigabitEthernet1/0/1] mpls ldp
[Router2-GigabitEthernet1/0/1] quit	[Router3-GigabitEthernet1/0/1] quit
# 配置 LSP 的触发建立策略	# 配置 LSP 的触发建立策略
[Router2] mpls	[Router3] mpls
[Router2-mpls] lsp-trigger all	[Router3-mpls] lsp-trigger all
[Router2-mpls] quit	[Router3-mpls] quit
配置 OSPF，通告各接口所连网段 IP 地址和 LSR ID 主机路由	配置 OSPF，通告各接口所连网段 IP 地址和 LSR ID 主机路由
[Router2] ospf 1	[Router3] ospf 1
[Router2-ospf-1] area 0	[Router3-ospf-1] area 0
[Router2-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255	[Router3-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255
[Router2-ospf-1-area-0.0.0.0] network 1.1.1.0 0.0.0.255	[Router3-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.255
[Router2-ospf-1-area-0.0.0.0] network 7.7.7.7 0.0.0.0	[Router3-ospf-1-area-0.0.0.0] network 8.8.8.8 0.0.0.0
[Router2-ospf-1-area-0.0.0.0] quit	[Router3-ospf-1-area-0.0.0.0] quit
[Router2-ospf-1] quit	[Router3-ospf-1] quit

在 MPLS LSP 回注中，LSP 的建立是基于 LDP（Label Distribution Protocol，标签分发协议）动态协商完成的，LDP 规定了标签分发过程中的各种消息以及相关的处理过程。LSR 之间将依据本地转发表中对应于一个特定 FEC 的入标签、下一跳节点、出标签等信息联系在一起，从而形成 LSP。所以在配置时，流量回注路径上的所有路由设备和相关接口上都需要配置 MPLS 和 LDP 功能。同时，在清洗设备和接入防护对象的路由设备上配置触发建立 LSP 的策略的命令 lsp-trigger all，让不同 FEC 触发建立 LSP 通道，清洗后的流量通过此通道完成回注。

7. MPLS VPN 回注

目前 MPLS 在网络中最常用的用法还是在应用于 VPN 中。如果在加入清洗设备之前，网络中有已经有相关 MPLS VPN 的部署，在加入清洗设备后，清洗后的流量可以通过配置 MPLS VPN 来进行回注。

MPLS VPN 是一个 L3VPN 技术，它使用 BGP 在网络中发布 VPN 路由，使用 MPLS 转发 VPN 报文。与 MPLS LSP 回注类似，清洗后的流量通过标签转发，不过，在 MPLS VPN 回注中，转发的报文带有两层标签，外层标签通过运行 LDP 来分配，指示如何到

达 BGP 下一跳；内层标签由 MP-BGP 来分配，表示报文的出接口或者属于哪个 VPN。

在图 6-12 中，清洗设备作为 Ingress PE（Provider Edge）设备，Router3 作为 Egress PE 设备，双方建立 MPLS VPN，清洗后的流量通过此 VPN 隧道完成回注。

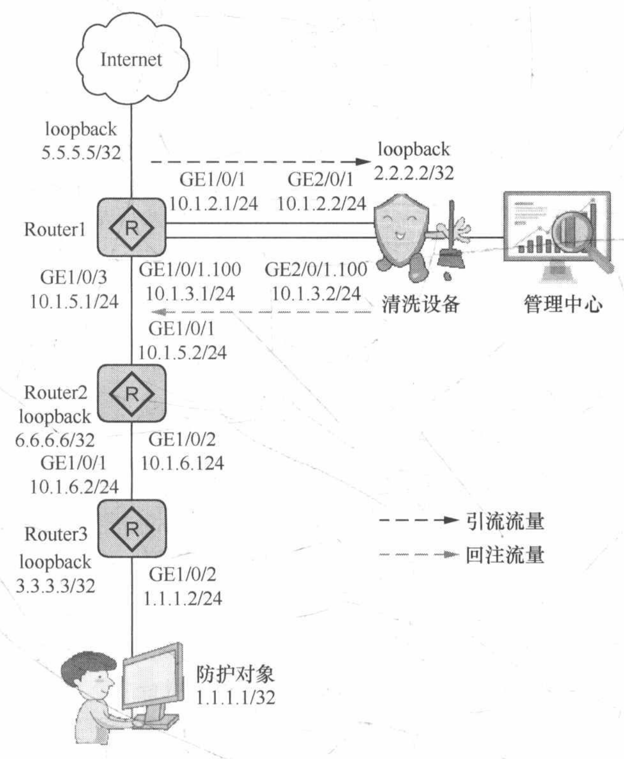


图 6-12　MPLS VPN 回注

建立 MPLS VPN，首先需要在清洗设备和 Router3 上要创建 VPN 实例，并且要在清洗设备和 Router3 上分别将引流接口和接入防护对象的接口加入各自的 VPN 实例中。其次，在回注的路径的所有 PE 和 P（Provider）设备（Router1、Router2）及相关接口上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。最后，在清洗设备和 Router3 上建立 MP-IBGP 对等体关系，使两 PE 之间传递 VPNv4 路由信息，实现 VPN 实例间的通信。具体的配置见表 6-11。

表 6-11　　MPLS VPN 回注关键配置

清洗设备	Router3
在清洗设备上，配置生成动态路由时使用的下一跳地址 <sysname> system-view [sysname] firewall ddos bgp-next-hop 10.1.2.1 对生成的 32 位主机 UNR 进行 FIB 过滤 [sysname] firewall ddos bgp-next-hop fib-filter 创建 VPN 实例，并在清洗设备上配置 BGP 功能及团体属性 [sysname] ip vpn-instance ddos	配置 Router3 的 loopback 地址 [Router3] interface loopback 1 [Router3-LoopBack1] ip address 3.3.3.3 32 [Router3-LoopBack1] quit 配置 MPLS # 配置 MPLS 基本功能 [Router3] mpls lsr-id 3.3.3.3 [Router3] mpls [Router3-mpls] quit

（续表）

清洗设备	Router3
[sysname-vpn-instance-ddos] ipv4-family [sysname-vpn-instance-ddos-af-ipv4] route-distinguisher 1:1 [sysname-vpn-instance-ddos-af-ipv4] vpn-target 1:1 import-extcommunity [sysname-vpn-instance-ddos-af-ipv4] quit [sysname-vpn-instance-ddos] quit [sysname] ip ip-prefix ipx index 10 permit 3.3.3.3 32 [sysname] route-policy 1 deny node 1 [sysname-route-policy] if-match ip next-hop ip-prefix ipx [sysname-route-policy] quit [sysname] route-policy 1 permit node 5 [sysname-route-policy] apply community no-advertise [sysname-route-policy] quit [sysname] route-policy 3 deny node 0 [sysname-route-policy] quit [sysname] bgp 200 [sysname-bgp] ipv4-family vpn-instance ddos [sysname-bgp-ddos] import-route unr [sysname-bgp-ddos] peer 10.1.2.1 as-number 100 [sysname-bgp-ddos] peer 10.1.2.1 route-policy 1 export [sysname-bgp-ddos] peer 10.1.2.1 route-policy 3 import [sysname-bgp-ddos] peer 10.1.2.1 advertise-community [sysname-bgp-ddos] quit [sysname-bgp] quit 在清洗设备的清洗口开启流量统计功能 [sysname] interface GigabitEthernet 2/0/1 [sysname-GigabitEthernet2/0/1] anti-ddos flow-statistic enable [sysname-GigabitEthernet2/0/1] quit 配置清洗设备的 loopback 地址 [sysname] interface loopback 1 [sysname-LoopBack1] ip address 2.2.2.2 32 [sysname-LoopBack1] quit 在清洗设备上配置 MPLS 功能，实现回注功能 # 配置 MPLS 基本功能 [sysname] mpls lsr-id 2.2.2.2 [sysname] mpls [sysname-mpls] quit [sysname] mpls ldp [sysname-ldp] quit [sysname] interface GigabitEthernet 2/0/1.100 [sysname-GigabitEthernet2/0/1.100] mpls [sysname-GigabitEthernet2/0/1.100] mpls ldp [sysname-GigabitEthernet2/0/1.100] quit # 配置接口绑定 VPN 实例	[Router3] mpls ldp [Router3-ldp] quit [Router3] interface GigabitEthernet 1/0/1 [Router3-GigabitEthernet1/0/1] mpls [Router3-GigabitEthernet1/0/1] mpls ldp [Router3-GigabitEthernet1/0/1] quit # 创建 VPN 实例，并配置接口绑定 VPN 实例 [Router3] ip vpn-instance ddos [Router3-vpn-instance-ddos] route-distinguisher 1:1 [Router3-vpn-instance-ddos] vpn-target 1:1 export-extcommunity [Router3-vpn-instance-ddos] vpn-target 1:1 import-extcommunity [Router3-vpn-instance-ddos] quit [Router3] interface GigabitEthernet 1/0/2 [Router3-GigabitEthernet1/0/2] ip binding vpn-instance ddos [Router3-GigabitEthernet1/0/2] ip address 1.1.1.2 255.255.255.0 [Router3-GigabitEthernet1/0/2] quit # 在清洗设备和 Router3 之间配置 MP-IBGP，使设备之间可以传播 VPNv4 路由 [Router3] bgp 200 [Router3-bgp] peer 2.2.2.2 as-number 200 [Router3-bgp] peer 2.2.2.2 connect-interface LoopBack 1 [Router3-bgp] ipv4-family vpnv4 [Router3-bgp-af-vpnv4] peer 2.2.2.2 enable [Router3-bgp-af-vpnv4] quit [Router3-bgp] quit # 将防护对象 IP 地址通过 BGP 发布出去 [Router3] bgp 200 [Router3-bgp] ipv4-family vpn-instance ddos [Router3-bgp-ddos] network 1.1.1.0 255.255.255.0 [Router3-bgp-ddos] quit [Router3-bgp] quit # 配置静态路由 [Router3] ip route-static vpn-instance ddos 0.0.0.0 0.0.0.0 10.1.6.1 public # 配置 LSP 的触发建立策略 [Router3] mpls [Router3-mpls] lsp-trigger all [Router3-mpls] quit 配置 OSPF，通告各接口所连网段 IP 地址和 LSR ID 主机路由 [Router3] ospf 1

（续表）

清洗设备	Router3
[sysname] interface GigabitEthernet 2/0/1 [sysname-GigabitEthernet2/0/1] ip binding vpn-instance ddos [sysname-GigabitEthernet2/0/1] ip address 10.1.2.2 255.255.255.0 [sysname-GigabitEthernet2/0/1] quit # 将接口 GigabitEthernet2/0/1 加入安全区域 [sysname] firewall zone trust [sysname-zone-trust] add interface GigabitEthernet 2/0/1 [sysname-zone-trust] quit # 在清洗设备和 Router3 之间配置 MP-IBGP，使设备之间可以传播 VPNv4 路由 [sysname] bgp 200 [sysname-bgp] peer 3.3.3.3 as-number 200 [sysname-bgp] peer 3.3.3.3 connect-interface LoopBack 1 [sysname-bgp] ipv4-family vpnv4 [sysname-bgp-af-vpnv4] peer 3.3.3.3 enable [sysname-bgp-af-vpnv4] peer 3.3.3.3 route-policy 3 export [sysname-bgp-af-vpnv4] quit [sysname-bgp] quit # 配置 LSP 的触发建立策略 [sysname] mpls [sysname-mpls] lsp-trigger all [sysname-mpls] quit 配置 OSPF，通告各接口所连网段 IP 地址和 LSR ID 主机路由 [sysname] ospf 1 [sysname-ospf-1] area 0 [sysname-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255 [sysname-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0 [sysname-ospf-1-area-0.0.0.0] quit [sysname-ospf-1] quit	[Router3-ospf-1] area 0 [Router3-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255 [Router3-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0 [Router3-ospf-1-area-0.0.0.0] quit [Router3-ospf-1] quit
Router1	**Router2**
配置 Router1 的 BGP 功能 [Router1] bgp 100 [Router1-bgp] peer 10.1.2.2 as-number 200 [Router1-bgp] quit 配置 Router1 的 loopback 地址 [Router1] interface loopback 1 [Router1-LoopBack1] ip address 5.5.5.5 32 [Router1-LoopBack1] quit 配置 MPLS # 配置 MPLS 基本功能 [Router1] mpls lsr-id 5.5.5.5 [Router1] mpls	配置 Router2 的 loopback 地址 [Router2] interface loopback 1 [Router2-LoopBack1] ip address 6.6.6.6 32 [Router2-LoopBack1] quit 配置 MPLS # 配置 MPLS 基本功能 [Router2] mpls lsr-id 6.6.6.6 [Router2] mpls [Router2-mpls] quit [Router2] mpls ldp [Router2-ldp] quit [Router2] interface GigabitEthernet 1/0/1

（续表）

Router1	Router2
[Router1-mpls] quit [Router1] mpls ldp [Router1-ldp] quit [Router1] interface GigabitEthernet 1/0/1.100 [Router1-GigabitEthernet1/0/1.100] mpls [Router1-GigabitEthernet1/0/1.100] mpls ldp [Router1-GigabitEthernet1/0/1.100] quit [Router1] interface GigabitEthernet 1/0/3 [Router1-GigabitEthernet1/0/3] mpls [Router1-GigabitEthernet1/0/3] mpls ldp [Router1-GigabitEthernet1/0/3] quit 配置 OSPF，通告各接口所连网段 IP 地址和 LSR ID 主机路由 [Router1] ospf 1 [Router1-ospf-1] area 0 [Router1-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255 [Router1-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255 [Router1-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0 [Router1-ospf-1-area-0.0.0.0] quit [Router1-ospf-1] quit	[Router2-GigabitEthernet1/0/1] mpls [Router2-GigabitEthernet1/0/1] mpls ldp [Router2-GigabitEthernet1/0/1] quit [Router2] interface GigabitEthernet 1/0/2 [Router2-GigabitEthernet1/0/2] mpls [Router2-GigabitEthernet1/0/2] mpls ldp [Router2-GigabitEthernet1/0/2] quit 配置 OSPF，通告各接口所连网段 IP 地址 [Router2] ospf 1 [Router2-ospf-1] area 0 [Router2-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255 [Router2-ospf-1-area-0.0.0.0] network 10.1.6.0 0.0.0.255 [Router2-ospf-1-area-0.0.0.0] network 6.6.6.6 0.0.0.0 [Router2-ospf-1-area-0.0.0.0] quit [Router2-ospf-1] quit 配置静态路由 [Router2] ip route-static 0.0.0.0 0.0.0.0 10.1.5.1

前面详细介绍过 BGP 引流的配置，在 ATIC 还需要进行相关设置，此处不再赘述。由于 BGP 引流以及 MPLS VPN 配置的需要，清洗设备与 Router1 和 Router3 都要建立 BGP 对等体关系，各设备学习到的路由会相互发布，如果控制不好，可能会引起路由环路等问题，所以我们需要做严格的控制。

在清洗设备的配置中，我们可以看到配置了 3 个策略控制内容，各自的含义都不相同。

```
[sysname] route-policy 1 permit node 5
[sysname-route-policy] apply community no-advertise
[sysname-route-policy] quit
[sysname] bgp 200
[sysname-bgp] ipv4-family vpn-instance ddos
[sysname-bgp-ddos] peer 10.1.2.1 as-number 100
[sysname-bgp-ddos] peer 10.1.2.1 route-policy 1 export
[sysname-bgp-ddos] peer 10.1.2.1 advertise-community
```

配置这段命令的作用是让 Router1 接收到清洗设备发布的路由后，不再向其他对等体发布。比如，Router1 如果还与其他设备建立了 BGP 对等体关系，那么它的对等体上是看不到清洗设备发布给 Router1 的路由的。这是因为清洗设备发布给 Router1 路由只用于 BGP 引流，对 Router1 以外的设备毫无作用，并且一旦被其他设备接收了，还有可能引起路由环路等问题。

```
[sysname] ip ip-prefix ipx index 10 permit 3.3.3.3 32
[sysname] route-policy 1 deny node 1
[sysname-route-policy] if-match ip next-hop ip-prefix ipx
[sysname-route-policy] quit
[sysname] bgp 200
[sysname-bgp] ipv4-family vpn-instance ddos
```

```
[sysname-bgp-ddos] peer 10.1.2.1 as-number 100
[sysname-bgp-ddos] peer 10.1.2.1 route-policy 1 export
```

这一段配置的作用是让清洗设备收到 Router3 发布的防护对象的路由后，不再发布给 Router1。因为清洗设备已经生成一条到防护对象的 UNR，并通过 BGP 发布给 Router1 作为引流使用，如果 Router1 再接收清洗设备从 Router3 学习到的到防护对象的 BGP 路由，可能对引流等造成影响。

```
[sysname] route-policy 3 deny node 0
[sysname-route-policy] quit
[sysname] bgp 200
[sysname-bgp] ipv4-family vpn-instance ddos
[sysname-bgp-ddos] peer 10.1.2.1 as-number 100
[sysname-bgp-ddos] peer 10.1.2.1 route-policy 3 import
```

此策略配置的作用是让清洗设备不接收 Router1 发布过来的路由，原因是清洗设备只用于流量引流并完成清洗，最后将清洗后的流量回注回去。从 Router1 发布过来的 BGP 路由对清洗设备没有任何作用，所以在清洗设备上要过滤掉这部分路由。

关于其他的配置，部分内容与 MPLS LSP 回注相同，且比较容易理解，在此不再多做讲解。

6.2.2 使用场景对比

以上为几种主要的回注方法相关配置及应用的介绍。表 6-12 是对这几种方法在使用场景方面的一个简单对比。

表 6-12　　回注方式对比

<table>
<tr><th>对比项</th><th>二层回注</th><th>静态路由回注（包括 UNR）</th><th>策略路由回注</th><th>GRE tunnel 回注</th><th>MPLS LSP 回注</th><th>MPLS VPN 回注</th></tr>
<tr><td rowspan="2">适用场景</td><td rowspan="2">仅限于回注口与防护对象处于同一网段时使用。一般用于 IDC 的二层组网</td><td>一般用于只有一个回注口的情况</td><td>一般用于存在多个回注口的情况</td><td>DDoS 清洗中心跨 AS 运营时使用较多</td><td colspan="2" rowspan="2">适用于回注路由器较多的复杂网络。要求相关路由器都支持 MPLS 或 MPLS VPN 功能</td></tr>
<tr><td colspan="3">当回注路由器较多或网络变化频繁时，这几个回注配置工作量大，维护麻烦，不建议使用</td></tr>
</table>

在实际场景中，应该以客户的实际需求和网络部署情况综合考虑，选择较为合适的方法来完成流量的回注。

6.3 引流回注

前面介绍了 Anti-DDoS 解决方案引流回注的实现，但配置完成并不能确保引流回注功能的可用。本节将通过对引流和回注功能的验证，来排查路由器、检测设备、清洗设备和 ATIC 的各项配置是否正确。

在组网中包括一个外网 PC，一个内网 Web 服务器。Anti-DDoS 检测设备和清洗设备旁路部署在组网中，对到达防护对象的流量进行检测和清洗。我们从外网 PC 向内网 Web 服务器发送 SYN 报文，通过对 Anti-DDoS 设备及 ATIC 进行配置，验证引流和回注功能配置的正确性。

6.3.1 前期准备

引流回注组网示意图如图 6-13 所示。

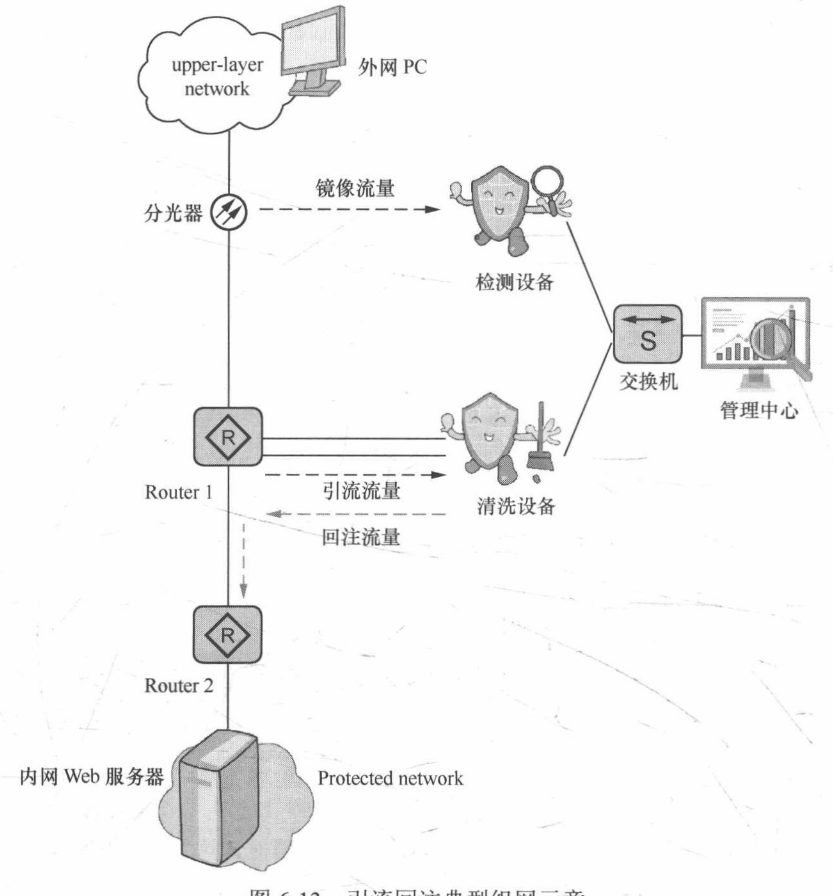


图 6-13 引流回注典型组网示意

6.3.2 测试思路

测试思路如下。

① 检测设备配置的 SYN flood 防御阈值为 1，当开始发送 SYN 报文后，流量超过检测设备的阈值，触发检测设备发送异常告警给 ATIC。

② 配置 Router1 和清洗设备的 BGP 功能，ATIC 下发至清洗设备的引流策略，会通过 BGP 发送给 Router1。Router1 会将到达 Web 服务器的流量引向 Anti-DDoS 清洗设备进行引流清洗。

③ Anti-DDoS 接收到内网的流量进行清洗后，再通过接口的策略路由，把正常流量回注给路由器，路由器通过策略路由将报文转发至交换机，最后到达 Web 服务器。

④ 反向的流量不经过 Anti-DDoS 设备，而是直接从路由器发送出去。

6.3.3 测试步骤

步骤 1 通过外网 PC 可以成功访问内网 Web 服务器。

步骤 2 将内网 Web 服务器 IP 地址加入防护对象，关联 Anti-DDoS 检测设备和清洗设备。

① 选择“防御 > 策略配置 > 防护对象”，在“防护对象列表”界面，单击“创建”，配置防护对象的基本信息，如图 6-14 所示。其中，“类型”包括“自定义”和“默认”两种。“名称”为防护对象名称，作为防护对象账号的补充，方便查看；“描述”为描述信息，用于备注此防护对象的详细信息。

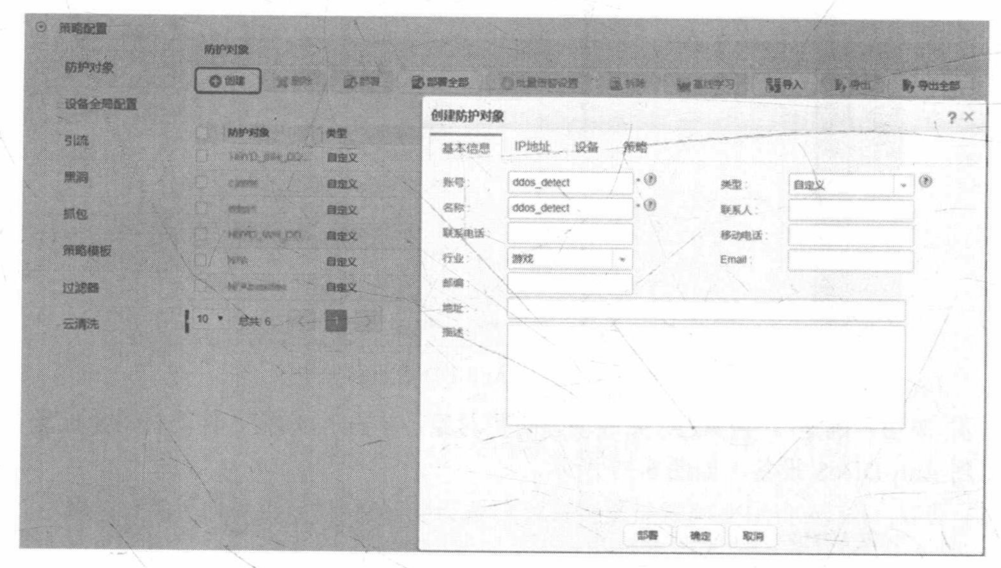


图 6-14 创建防护对象

② 在“创建防护对象”界面，单击“IP 地址”页签，单击“创建”，配置自定义防护对象的 IP 地址，如图 6-15 所示。

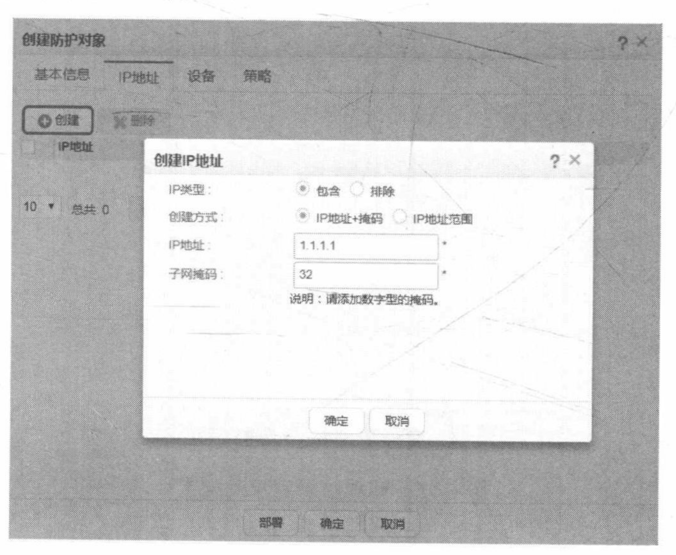


图 6-15 配置防护对象 IP 地址

③ 单击“设备”页签，为防护对象关联 Anti-DDoS 设备，选中设备前的复选框，单击“确定”，如图 6-16 所示。

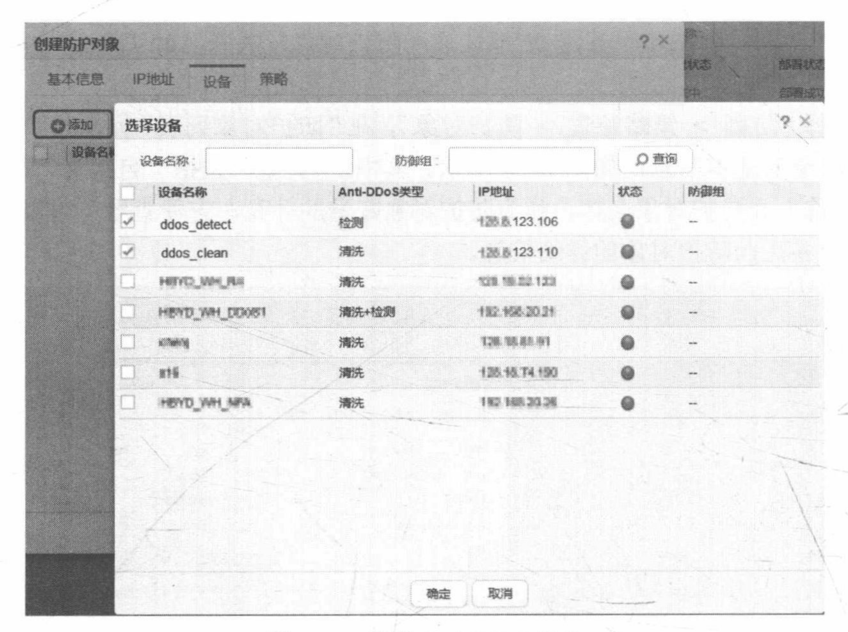


图 6-16　关联 Anti-DDoS 设备

④ 单击“确定”，在 ATIC 完成创建防护对象，单击“部署”，将防护对象配置直接部署到 Anti-DDoS 设备，如图 6-17 所示。

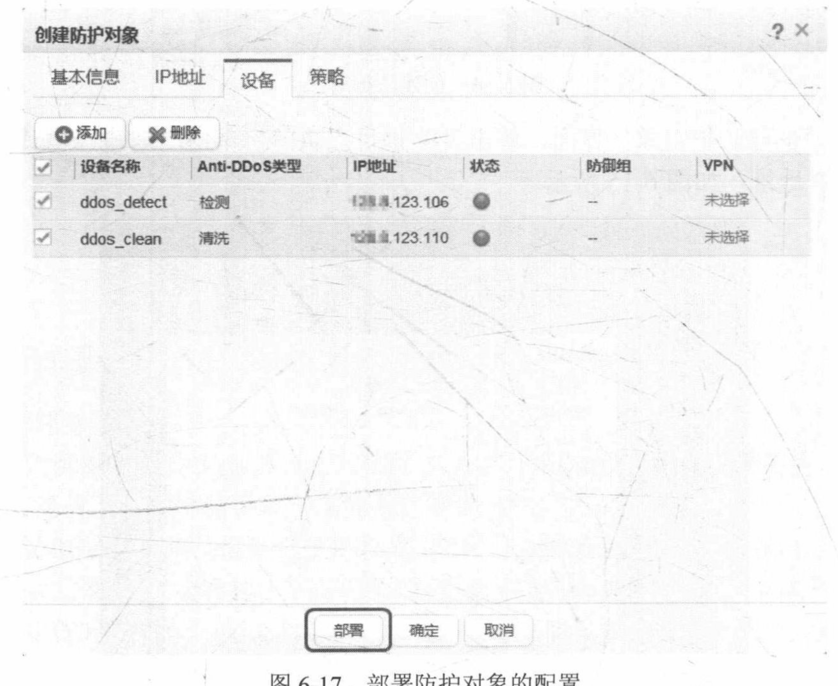


图 6-17　部署防护对象的配置

⑤ 在“防护对象列表”界面，确保部署状态显示为“部署成功”。

步骤 3　修改检测设备的 SYN flood 防御阈值为 1，修改清洗设备的 SYN flood 防御阈值为 1。

① 选择“防御>策略配置>防护对象”，单击防护对象对应的，将引流模式和防御

模式修改为“自动执行”，如图 6-18 所示。

图 6-18　防御模式的配置

引流模式的“自动执行”是指检测设备检测到流量异常后上报给 ATIC，ATIC 自动生成引流任务，并自动下发引流任务到清洗设备。防御模式的“自动执行”是指清洗设备检测到流量异常后，生成异常事件并自动启用防御系统。

② 在“防御策略”页签中，单击“操作”列的⚙，选择“TCP”页签，修改检测设备的 SYN flood 防御阈值为 1，修改清洗设备的 SYN flood 防御阈值为 1，如图 6-19 所示。



图 6-19　SYN flood 防御阈值的配置

③ 如果部署状态变化为“部分部署”，则需要重新部署。

步骤 4 为了避免测试不产生任何效果，需要选择“防御 > 策略配置 > 防护对象”，单击防护对象对应的，修改“提示”动作为“启动引流”，允许小流量触发告警，如图 6-20 所示。

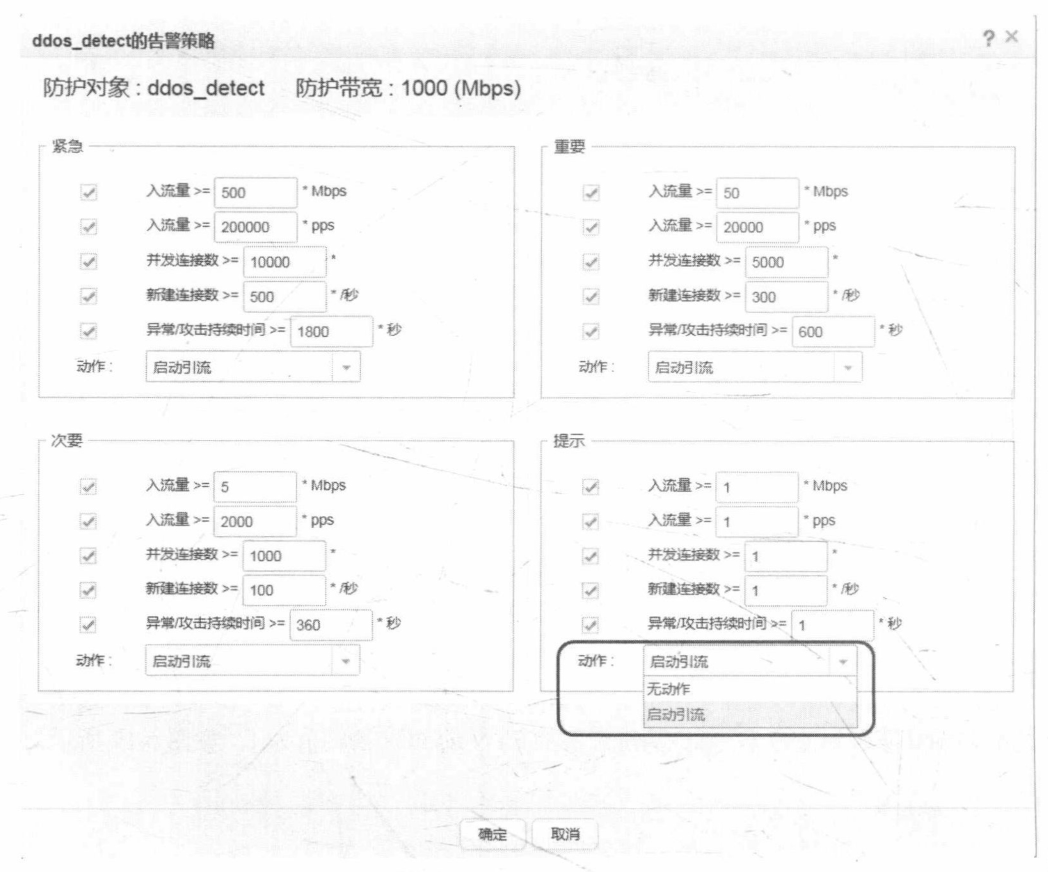


图 6-20 告警策略的配置

需要注意的是，为避免产生过多的告警，测试结束后需要将本步骤修改回来。

步骤 5 单击键盘 F5 按键，通过外网 PC 持续访问 Web 服务器。

6.3.4 期望的测试结果

步骤 1 ATIC 发现防护对象状态异常，点击进去后可以看到检测设备异常，如图 6-21 和图 6-22 所示。

步骤 2 单击键盘 F5 按键，持续发送 SYN 报文。

步骤 3 选择“报表 > 专项报表 > 流量分析”，选择“流量对比”页签，从下拉列表中选择检测设备或清洗设备，分别查看相对应的报表。

通过“流量对比”，可以了解在一定时间间隔内，指定设备的流量转发情况：如果选择的设备为清洗设备，则报表展示入流量、出流量、攻击流量和反弹流量信息；如果选择的设备为检测设备，则报表展示检测流量信息。我们在检测设备和清洗设备的报表

中都可以看到流量。

防护对象

创建　删除　部署　部署全部　批量告警设置　拆除　基线学习　导入　导出

防护对象	类型	设备名称	服务学习状态	基线学习状态	异常状态	防御状态
ddos_detect	自定义	ddos_detect	未学习	学习中	异常	自动防御
ddos_clean	自定义	ddos_clean	未学习	学习中	正常	--
[illegible]	自定义	[illegible]	未学习	学习中	正常	--
[illegible]	自定义	[illegible]	未学习	未学习	正常	--
[illegible]	自定义	[illegible]	未学习	学习中	正常	--
[illegible]	自定义	[illegible]	未学习	未学习	正常	--
[illegible]	自定义	[illegible]	未学习	学习中	正常	--

10　总共: 7　1

图 6-21　异常状态的显示

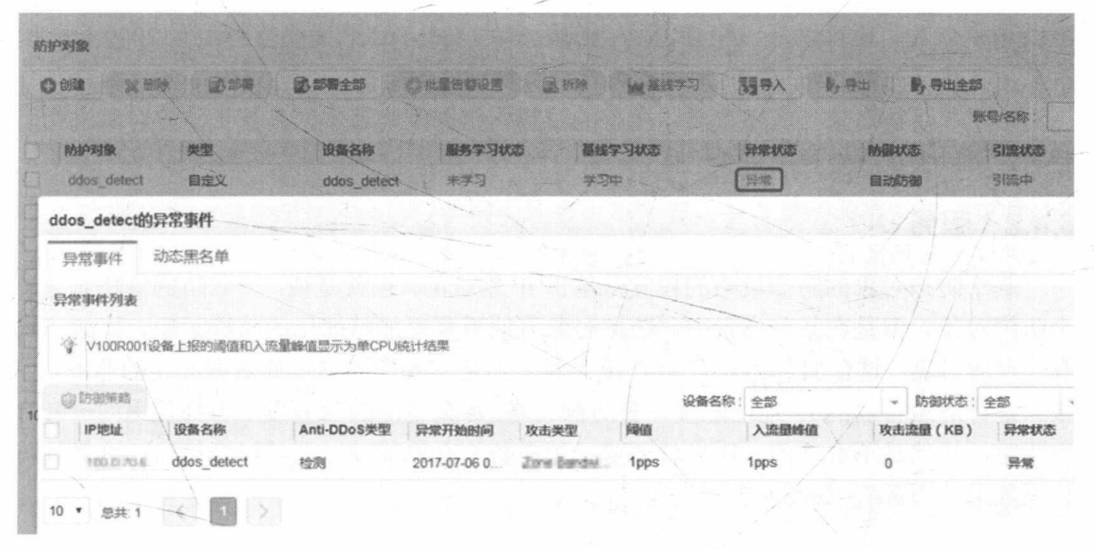


图 6-22　异常事件的详情

6.4　策略配置

6.4.1　防护对象

在介绍配置之前，我们先认识一个重要的名词——防护对象。

Anti-DDoS 设备是基于目的 IP 地址进行防护的。也就是说，Anti-DDoS 设备对到达

受保护客户 IP 方向的流量进行检测和清洗。我们通常把这个目的 IP 地址加入到一个 Zone，也就是“防护对象”中，如图 6-23 所示。

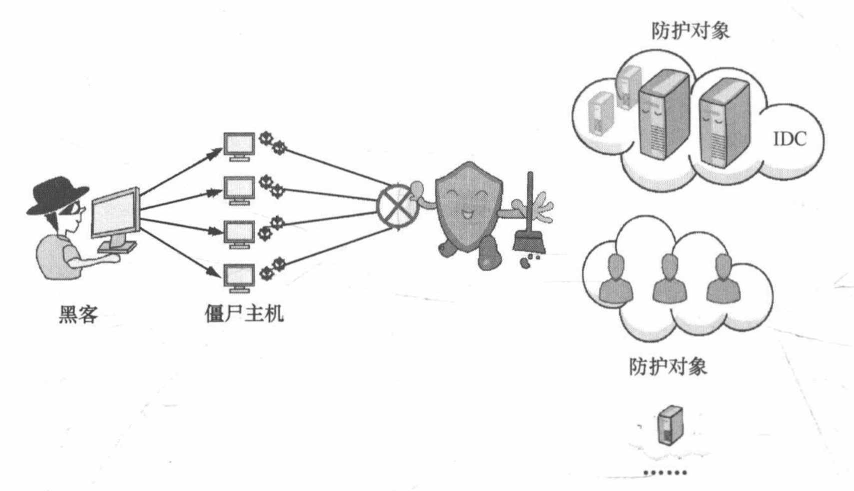


图 6-23 防护对象

防护对象里的 IP 地址都是需要保护的 IP 地址的集合，它可以是一个单独的 IP，也可以是多个 IP，还可以是一些 IP 段。当前版本的 Anti-DDoS 设备支持配置 2000 个防护对象，支持同时对 20 万个 IP 地址的流量进行精细化的防护。

这个“防护对象”非常重要，所有的精细化防御策略基本都是基于防护对象进行配置的，所以大家一定要理解并记住它。

6.4.2 服务

基于防护对象的防御策略的粒度是基于 IP 地址的，也就是说，一套防御策略对应一个防护对象。但是在某些场景中，防护对象可能需要更加精细化的防御策略。比如，我有一台服务器，这台服务器只有一个 IP 地址，但是它不同的端口处理着不同的业务。如果只是针对服务器的 IP 地址配置一套防御策略，那么不同的业务模型下都使用同一套防御策略，显然是不合理的。所以就需要一种在防护对象基础上更精细的策略，这就是防护对象的“服务”，如图 6-24 所示。

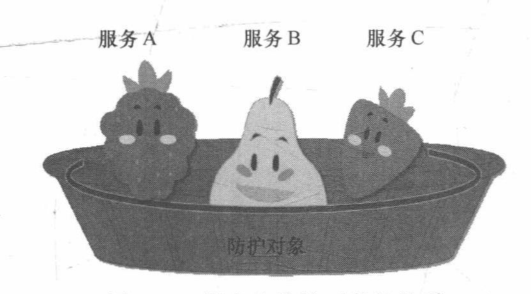


图 6-24 服务和防护对象的关系

服务是“目的 IP 地址+端口号”的集合，通过不同的端口号，区分不同的业务。

6.4.3 命令行配置与 ATIC 配置

华为的 Anti-DDoS 系统的防御策略是非常多样和精细化的，支持 ATIC 配置和命令行配置两种方式。大部分命令行支持的配置，在 ATIC 都有对应的 Web 界面。两者定位不同，命令行支持的配置是个全集，ATIC 支持的配置是部分基础的配置，而高级一点的防御策略，则只支持命令行配置，因此，就只能在 Anti-DDoS 设备上用命令行配置。一般都是有经验的运维工程师或资深管理员根据现网运维经验和实际网络情况对其进行调整，不建议普通管理员对其轻易开启。

在现网配置过程中，如果是 ATIC 支持的防御策略，则一定要由 ATIC 配置并下发到 Anti-DDoS 设备，而不要直接在 Anti-DDoS 设备上直接用命令行配置，否则可能会导致配置的冲突。

6.4.4 防御策略的配置

防御策略配置原则：为每一种可能的 DDoS 攻击配置防御策略，避免业务被任何一种 DDoS 攻击影响。

DDoS 攻击主要是占用网络带宽或者服务器资源，使服务器无法对外提供服务。

例如，对于一个 Web 网站，攻击者可以使用 UDP flood 拥塞网络，导致正常用户因为没有带宽而无法访问网站；攻击者也可以使用 HTTP flood 攻击网站，使服务器资源耗尽，导致正常用户无法访问网站。因此，一个 IP 地址可能会遭受到各种类型的 DDoS 攻击，它并不会因为服务器是 Web 服务器而仅遭到 HTTP 类的攻击。

因此，我们需要配置多种防御策略，防御任何可能遇到的 DDoS 攻击。

防御策略实质是针对各种协议类型的流量大小设置一个合理的阈值，作为正常流量的上限，当网络中的实际流量大小超过设置的阈值时，我们就会认为流量发生异常，触发相应的防御功能。

在配置防御策略前，管理员经常会面临两个疑问：

① 开启哪些类型的防御功能？

② 防御阈值应该设置为多少才合理？

接下来，我们就以上疑问来进行解答。

Anti-DDoS 系统最常用的场景就是保护各种服务器，这些服务器有的是 DNS 服务器，有的是 Web 服务。服务器不同，业务模型也不同，因此配置的防御策略就不同。

下面我们就从几种主流服务器的类型，说明防御策略的配置重点。

1. 通用服务器

当不能确定服务器服务类型时，可以采用通用策略模板，配置防御策略。

① 配置 TCP 通用防御策略。防御阈值可以根据基线学习的结果进行调整，如图 6-25 所示。

ACK Flood 防御：严格模式的防御效果优于宽松模式的效果。

- 在直路部署时，推荐使用严格模式，因为业务不会有中断，防御效果也要好于宽松模式的效果。
- 在旁路部署时，建议使用宽松模式，因为如果使用严格模式，根据严格模式防御

原理，业务被引流后，ACK 报文中的会话必须是由 SYN 或 SYN-ACK 建立，否则报文会被丢弃，会话需要重建后业务才会正常。

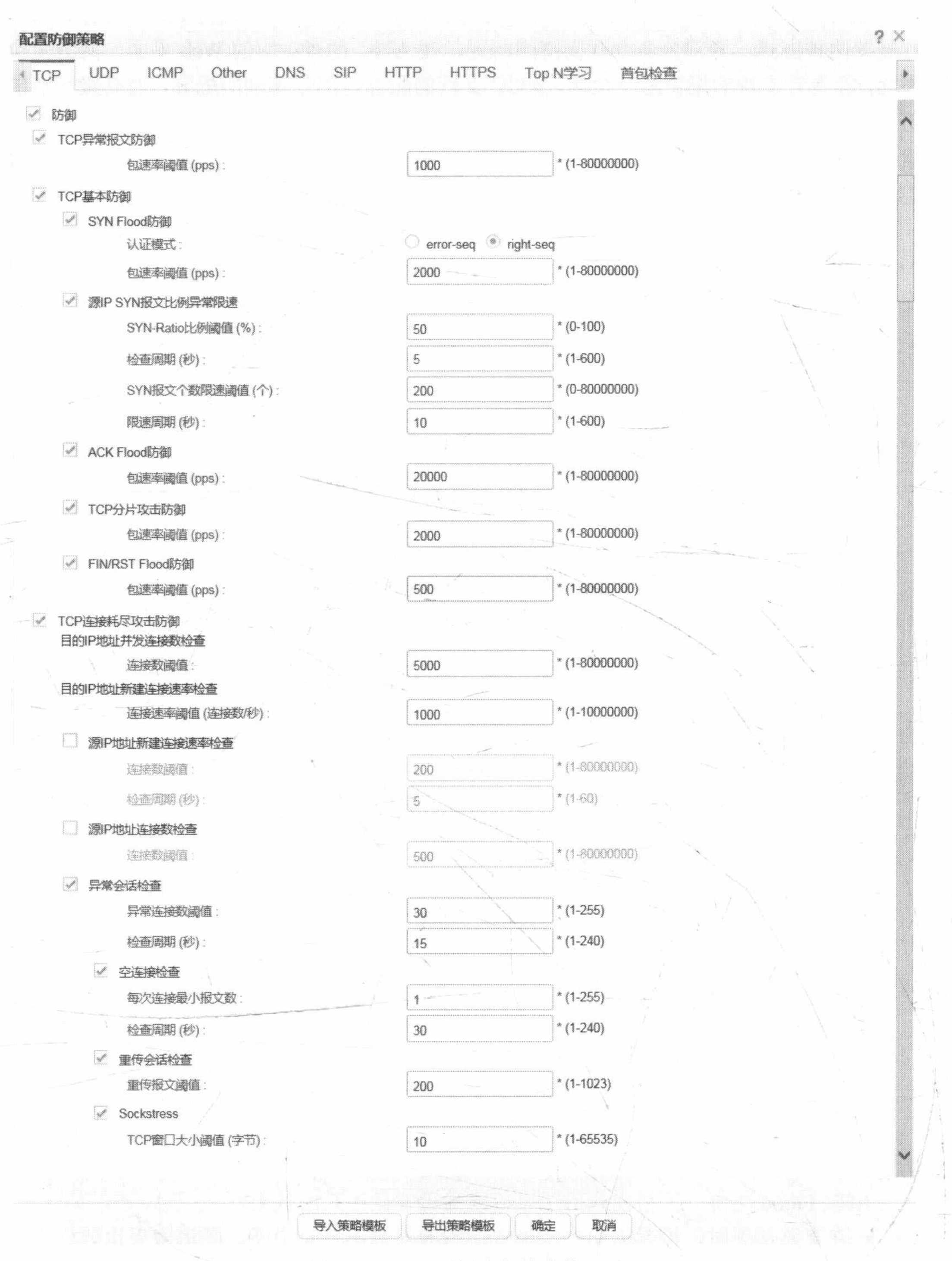


图 6-25 TCP 通用防御策略的配置

在攻击时，图 6-25 中的配置仅能告警，只有开启动态黑名单功能才能进行清洗，建议在应急的时候再开启动态黑名单功能，开启方法如图 6-26 所示。

LF默认防护对象的防御策略

防御模式　过滤器　位置策略　防御策略

防护带宽 (Mbps)：1000 *(1-2000000)　入流量超规格启动限流
过滤器丢弃阈值 (pps)：100 *(1-80000000)
引流模式：自动执行　手动确认
防御模式：自动执行　手动确认
动态黑名单模式：自动　关闭
单目的IP限流：开启　限流阈值 (Mbps)：100 *(1-2000000)
IP信誉：开启　告警阈值 (pps)：2000 *(1-80000000)
新建会话限速：开启　限速阈值 (连接数/秒)：30000 (1-400000)
秒级黑洞：开启　黑洞阈值 (Mbps)：100 (1-10000000)
恶意流量过滤：DoS攻击工具

确定　关闭

图 6-26　开启动态黑名单

② 配置 UDP 通用防御策略，如图 6-27 所示。



图 6-27　UDP 通用防御策略的配置

③ 配置 ICMP 通用防御策略，如图 6-28 所示。



图 6-28 ICMP 通用防御策略的配置

④ 配置 Other 协议通用防御策略，如图 6-29 所示。

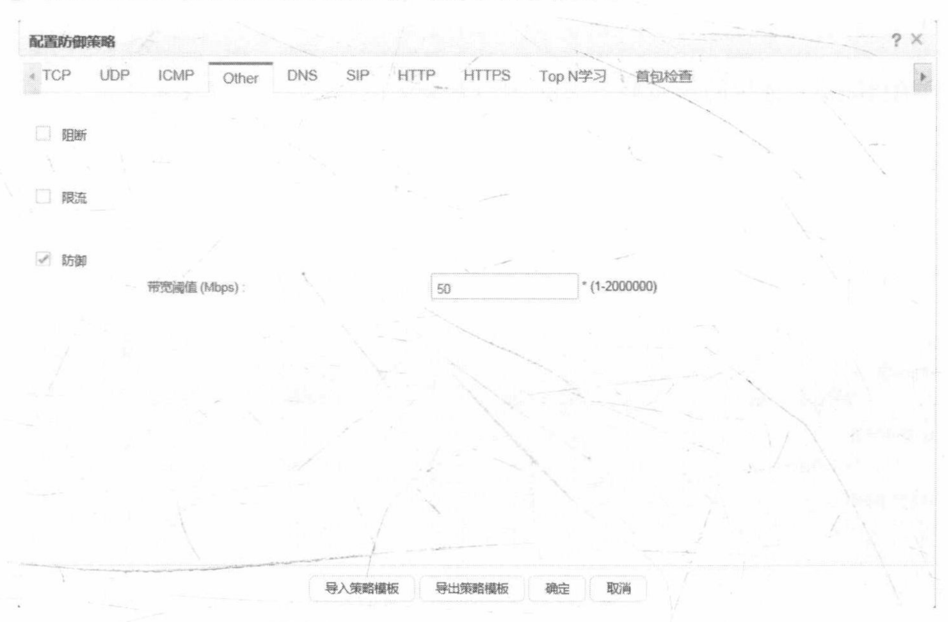


图 6-29 Other 协议通用防御策略的配置

- 如果可以确认访问被保护的网络流量只有 TCP、UDP、ICMP 业务，不包含 IPSec、GRE、IGMP 等其他 IP，建议开启限流，防御效果会更好。
- 如果存在 IPSec、GRE、IGMP 等其他 IP，则不能开启限流，否则会影响正常业务。

⑤ 配置 DNS 协议通用防御策略，如图 6-30 所示。

⑥ 配置 HTTP 通用防御策略，如图 6-31 所示。

多数用户的浏览器和 App 都有完整的 HTTP 栈，因此可以顺利通过“302 重定向”。

当流量超过阈值触发防御后，用户感知不到认证过程，业务访问不会受到任何影响；但少数的 App 和程序可能使用不完整的 HTTP 栈，无法通过 HTTP“302 重定向”的认证，导致业务受到影响，这个时候就需要关闭 HTTP 源认证防御，避免影响业务。

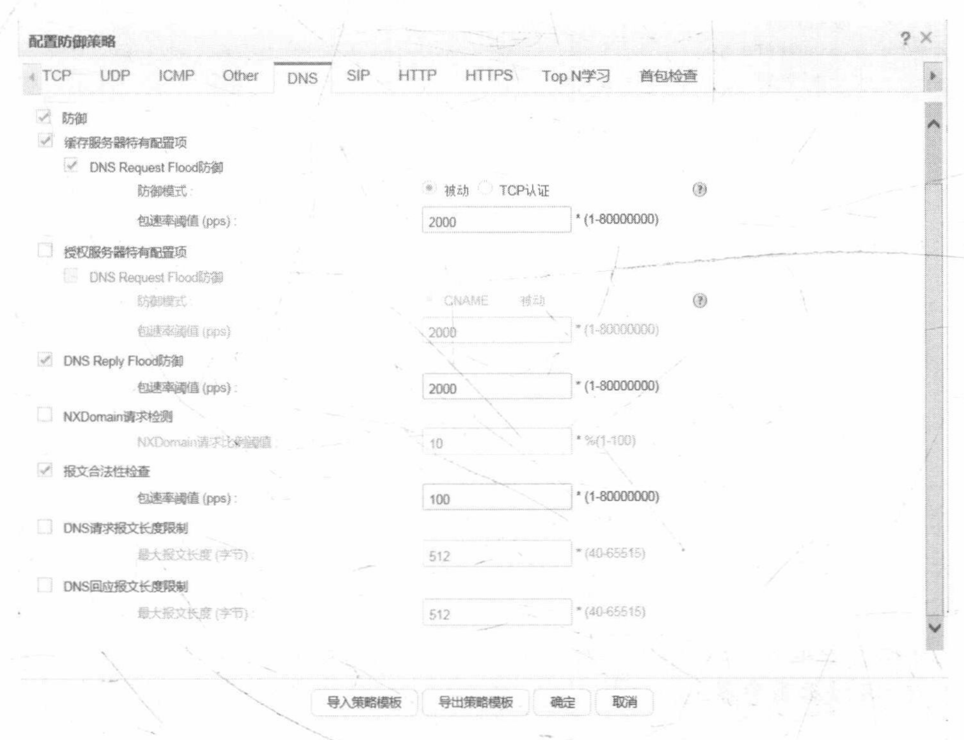


图 6-30　DNS 协议通用防御策略的配置

图 6-31　HTTP 通用防御策略的配置

⑦ 配置 HTTPS 协议通用防御策略，如图 6-32 所示。

配置防御策略

TCP UDP ICMP Other DNS SIP HTTP HTTPS Top N学习 首包检查

防御
HTTPS源认证防御
基于目的IP统计
包速率阈值 (pps)： 2000 * (1-80000000)
基于源IP统计
包速率阈值 (pps)： 0 * (0-80000000)
SSL防御
重协商最大次数： 3 * (1-10)
重协商检查周期 (秒)： 30 * (1-240)
异常会话最大数： 3 * (1-10)
异常会话检查周期 (秒)： 15 * (1-240)

导入策略模板 导出策略模板 确定 取消

图 6-32　HTTPS 协议通用防御策略的配置

⑧ 配置过滤器：对于不提供服务的端口，请管理员通过配置过滤器进行阻断，否则将会影响防御效果。

单击“过滤器”页签，单击 关联过滤器 ，选中 ATIC 缺省提供的全部常用的过滤器模板，单击“确定”。

2. DNS 缓存服务器

流量特点：DNS 缓存服务器主要承载 DNS 业务，DNS 业务以端口号为 53 和 5060 的 UDP 报文为主，由于其他端口的 UDP 业务和 TCP 业务报文较少，其他类型的报文也很少，因此精细化防御以 DNS 防御策略为主。

① TCP 防御：TCP 业务较少，配置以限速为主，如图 6-33 所示。

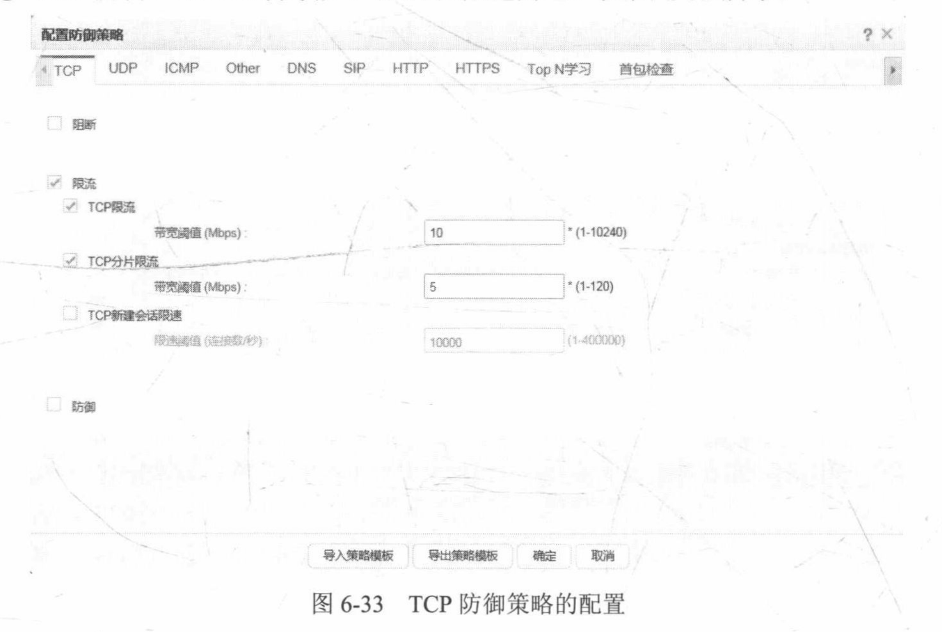


图 6-33　TCP 防御策略的配置

② UDP 防御：通常 DNS 服务器上除了 53 和 5060 以外的其他端口的 UDP 业务比较少，UDP 限速正是针对除 53 和 5060 以外的其他端口 UDP 进行的限速，所以限速功能可开启，如图 6-34 所示。

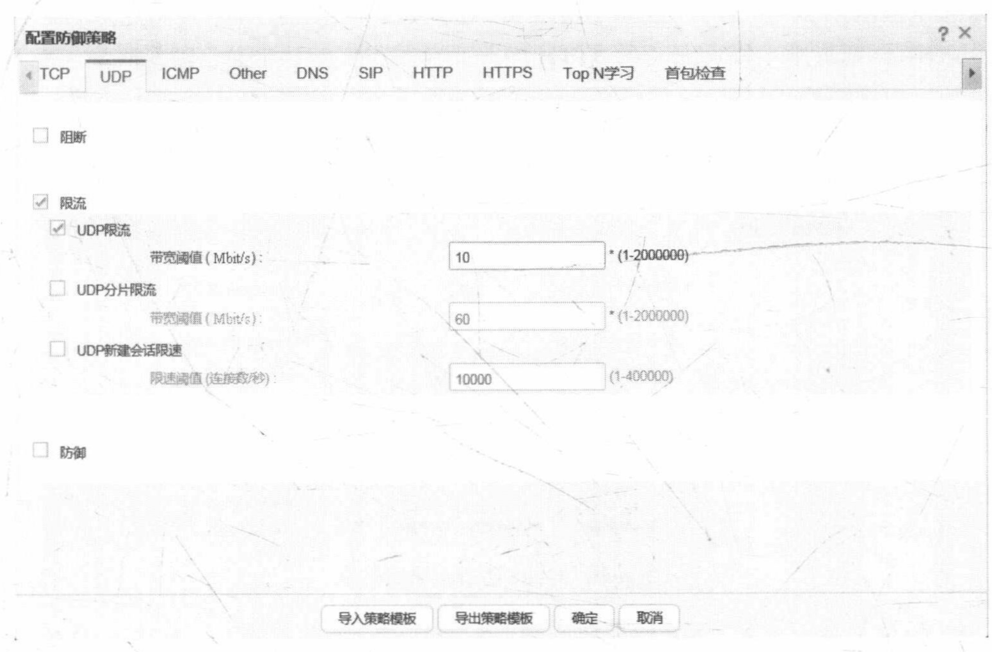


图 6-34　UDP 防御策略的配置

③ ICMP 防御：正常情况下，现网中只有少量的 Ping 报文，所以 ICMP 的限速阈值可以配置得小一点，如图 6-35 所示。



图 6-35　ICMP 防御策略的配置

④ Other 报文的防御策略以限流为主，如图 6-36 所示。

图 6-36 Other 防御策略的配置

⑤ DNS 防御：针对 DNS 服务器的类型配置精细化的防御策略，如图 6-37 所示。

图 6-37 DNS 防御策略的配置

⑥ HTTP 源认证防御；如图 6-38 所示。

多数用户的浏览器和 App 都有完整的 HTTP，因此可以顺利通过“302 重定向”认证，当流量超过阈值触发防御后，用户感知不到认证过程，业务访问不会受任何影响。但个别的 App 和程序可能使用不完整的 HTTP，无法通过 HTTP“302 重定向”的认证，导致业务受到影响，这个时候我们就需要关闭 HTTP 源认证防御，避免影响业务。

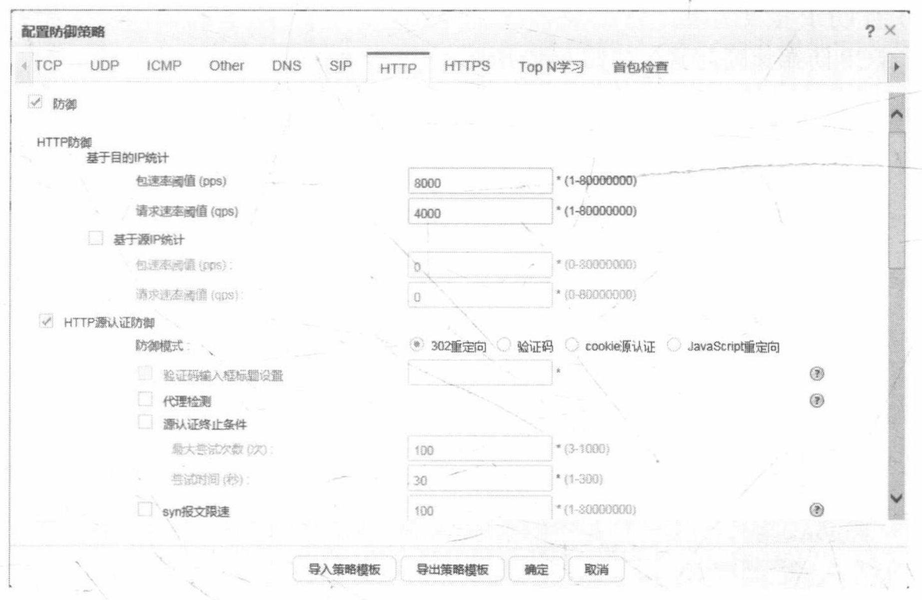


图 6-38　HTTP 防御策略的配置

⑦ HTTPS 源认证防御，如图 6-39 所示。



图 6-39　HTTPS 防御策略的配置

⑧ 过滤器配置：除上述防御策略以外，对于不提供服务的端口，我们可以通过配

置过滤器对其进行阻断。

我们单击“关联过滤器”，选中 ATIC 缺省提供的除“DNS_Amplification”外的所有过滤器模板，单击“确定”。

3. DNS 授权服务器

流量特点：DNS 授权服务器主要承载的是 DNS 业务，DNS 业务主要以端口号为 53 和 5060 的 UDP 报文为主。

① TCP 防御策略配置，如图 6-40 所示。

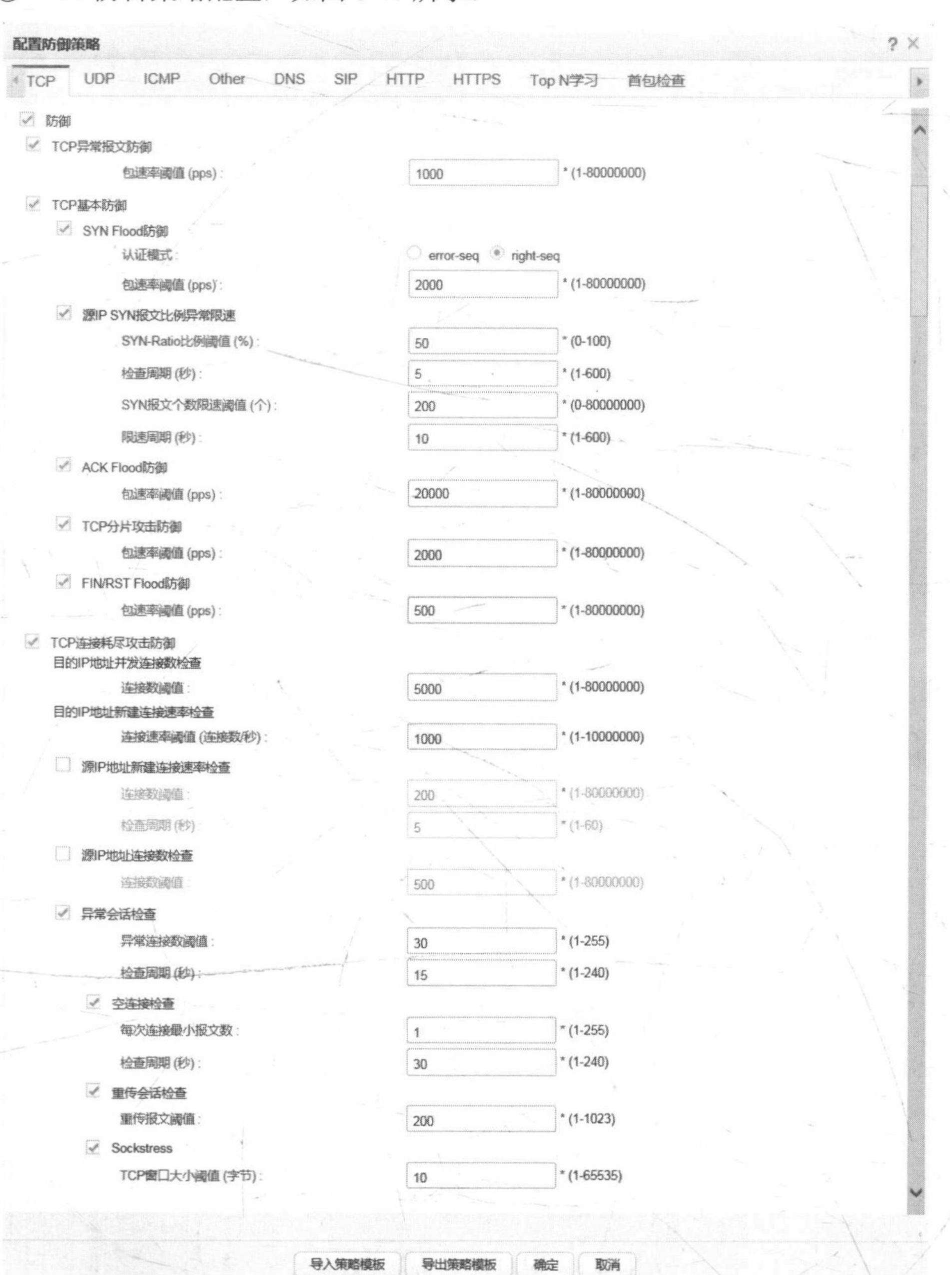


图 6-40 TCP 防御策略的配置

② UDP 防御：DNS 服务器上除了 53 和 5060 的 UDP 报文以外，其他端口 UDP 业务比较少。UDP 限速正是针对除 53 和 5060 的 UDP 报文以外的其他端口 UDP 业务进行的限速，如图 6-41 所示。

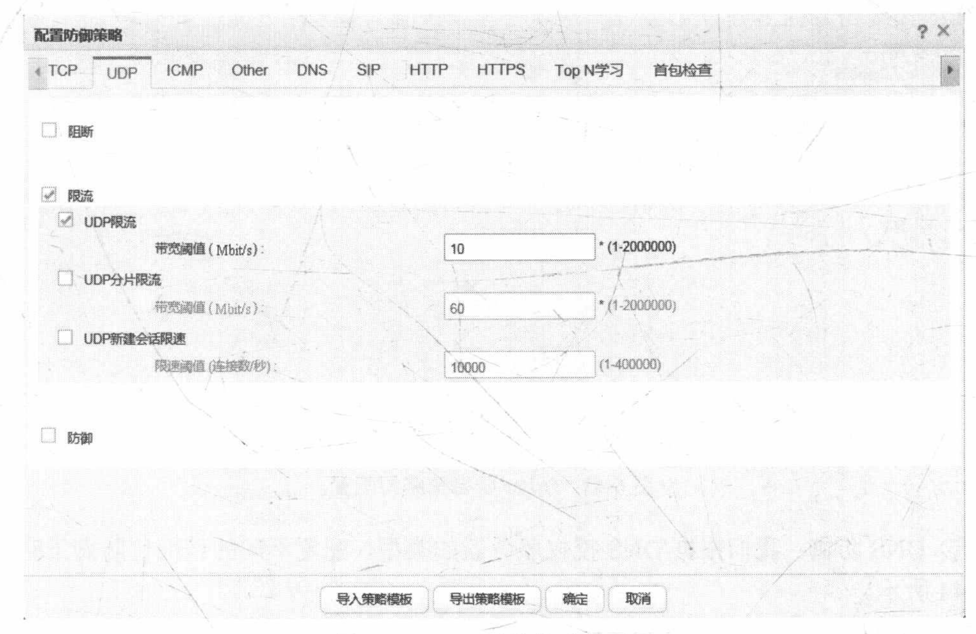


图 6-41 UDP 防御策略的配置

③ ICMP 防御：正常情况下现网中只有少量的 Ping 报文，所以 ICMP 的限速阈值可以配置得小一点，如图 6-42 所示。



图 6-42 ICMP 防御策略的配置

④ Other 报文的防御以限流为主，如图 6-43 所示。

图 6-43　Other 防御策略的配置

⑤ DNS 防御：我们根据 DNS 授权服务器的类型，配置不同的精细化防御策略，如图 6-44 所示。

图 6-44　DNS 防御策略的配置

⑥ HTTP 源认证防御，如图 6-45 所示。多数用户的浏览器和 App 都有完整的 HTTP，因此可以顺利通过“302 重定向”认证，当流量超过阈值触发防御后，用户感知不到认证过程，业务访问没有任何影响。但个别的 App 和程序可能使用不完整的 HTTP，无法通过 HTTP“302 重定向”的认证，导致业务受到影响，这个时候我们就需要关闭 HTTP 源认证防御，避免影响业务。

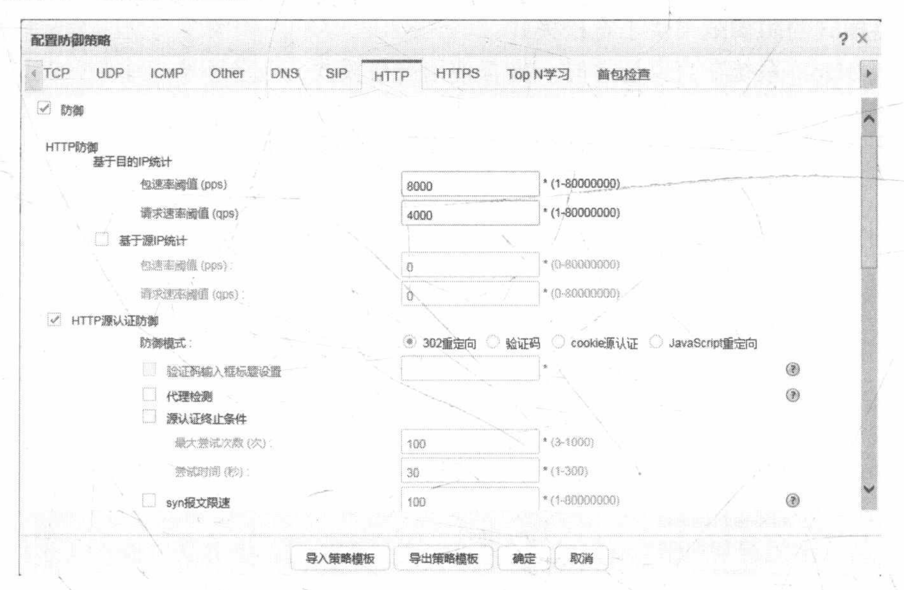


图 6-45　HTTP 防御策略的配置

⑦ HTTPS 源认证防御，如图 6-46 所示。



图 6-46　HTTPS 防御策略的配置

⑧ 过滤器配置：除上述防御策略外，对于不提供服务的端口，我们可以通过配置过滤器将其阻断。

我们单击“关联过滤器”，选中 ATIC 缺省提供的除“DNS_Amplification”外的所有过滤器模板，单击“确定”。

4．Web 服务器

流量特点：Web 服务器以 HTTP 和 HTTPS 业务为主，UDP 业务流量较少。

① TCP 防御：TCP 基本防御都可以开启，如图 6-47 所示。其中，ACK Flood 防御中的严格模式的防御效果优于宽松模式。

Anti-DDoS 系统在直路部署时，推荐使用严格模式，业务不会有中断，其防御效果也好于宽松模式的防御效果。

Anti-DDoS 系统在旁路部署时，建议使用宽松模式，因为如果在旁路部署时使用严格模式，根据严格模式防御原理，业务在引流后 ACK 报文命中的会话必须是由 SYN 或 SYN-ACK 建立，否则报文会被丢弃，会话重建后业务才会正常。

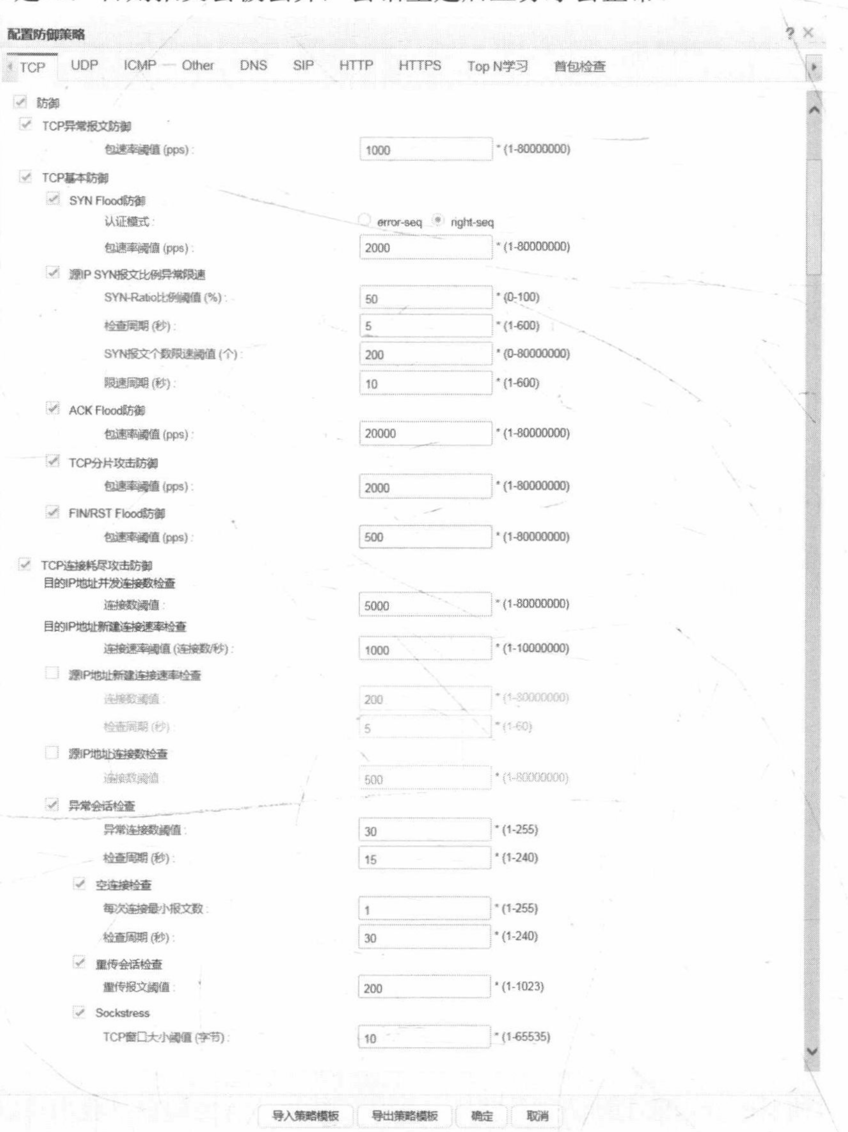


图 6-47 TCP 防御策略的配置

图 6-47 中的配置在攻击时仅能告警，我们需要配置动态黑名单功能才能进行清洗。建议在应急的时候再开启动态黑名单功能，开启方法如图 6-48 所示。

图 6-48 开启动态黑名单

② UDP 防御：Web 服务器一般没有 UDP 业务，因此 UDP 流量很小，直接限流即可，如图 6-49 所示。

图 6-49 UDP 防御策略的配置

③ ICMP 防御：正常情况下，现网中只有少量的 Ping 报文，因此 ICMP 的限速阈值可以配置得小一点，如图 6-50 所示。

图 6-50 ICMP 防御策略的配置

④ Other 报文的防御以限流为主，如图 6-51 所示。

图 6-51 Other 防御策略的配置

⑤ HTTP 源认证防御，如图 6-52 所示。

多数用户的浏览器和 App 都有完整的 HTTP，因此可以顺利通过“302 重定向”认证，当流量超过阈值触发防御后，用户感知不到认证过程，业务访问不会受任何影响。但个别的 App 和程序可能使用不完整的 HTTP，无法通过 HTTP“302 重定向”的认证，

导致业务受到影响，这个时候我们需要关闭 HTTP 源认证防御，避免影响业务。

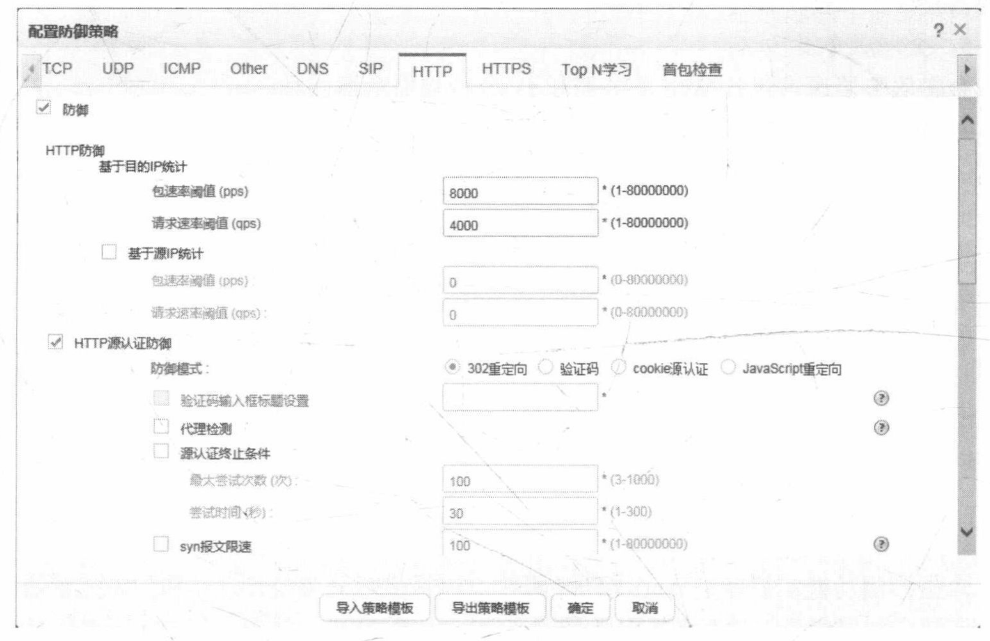


图 6-52　HTTP 防御策略的配置

⑥ HTTPS 源认证防御，如图 6-53 所示。



图 6-53　HTTPS 防御策略的配置

⑦ 过滤器配置：除上述防御策略以外，对于不提供服务的端口，我们可以通过配置过滤器对其进行阻断。

我们单击“关联过滤器”，选中 ATIC 缺省提供的除“DNS_Amplification”外的所有过滤器模板，单击“确定”。

5. 金融服务器

金融服务器通常包含 Web 服务器和 DNS 授权服务器两种。

① Web 服务器，其防御策略请参考“Web 服务器”的防御策略配置模板。

② DNS 授权服务器，其防御策略请参考“DNS 授权服务器”的防御策略配置模板。

6. 游戏服务器

游戏服务通常包含 3 种类型：Web 服务器、TCP 游戏服务器和 UDP 游戏服务器。

① Web 服务器，其防御策略请参考“Web 服务器”的防御策略配置模板。

② TCP 游戏服务器，其采用“通用服务器”的策略模板，其中 UDP 限流阈值调整为“10Mbit/s”。

③ UDP 游戏服务器，其采用“通用服务器”的策略模板，其中 TCP 防御调整为“限流”。

6.4.5 阈值调整

攻击检测功能实质就是 Anti-DDoS 系统对流量进行分类统计，并和预先配置的阈值进行比较，如果流量超过阈值则认为流量异常，上报 ATIC。因此，攻击判断是否准确取决于阈值设置的是否合理。然而，阈值的设置通常没有统一的经验值可循，不同的网络有不同的应用，每种应用又有不同的实际带宽。对于很多运维工程师来说，Anti-DDoS 系统上线后的阈值配置一直是个让人头疼的问题。

① 阈值设置过低，在没有发生攻击时，系统就启动攻击防御功能，会产生误报。

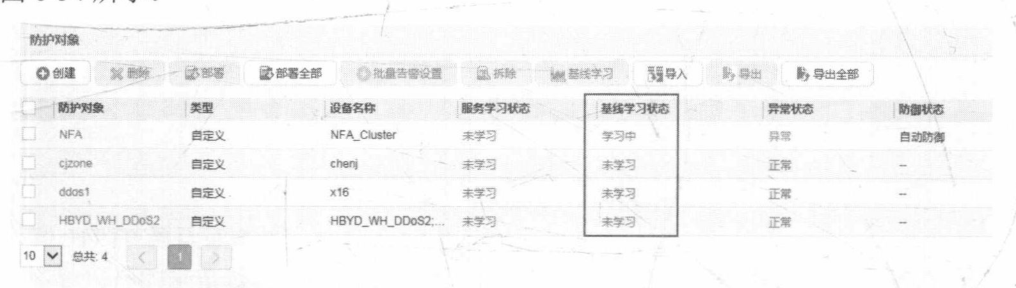
② 阈值设置过高，即使发生了攻击，系统也无法感知，不能及时启动防御功能。

管理员在配置防御阈值前，应该先了解网络中流量的基本模型，根据网络中流量模型手工配置防御阈值。

Anti-DDoS 系统支持对流量的动态基线学习功能。动态基线学习是指系统按时间统计用户网络流量，学习正常网络环境中一定时间间隔内的流量最高值，并以曲线形式在管理中心将其展现给管理员。

基线学习设置如下。

① 选择“防御→策略配置→防护对象”，单击具体防护对象的“基线学习状态”列，如图 6-54 所示。



防护对象	类型	设备名称	服务学习状态	基线学习状态	异常状态	防御状态
NFA	自定义	NFA_Cluster	未学习	学习中	异常	自动防御
cjzone	自定义	chenj	未学习	未学习	正常	--
ddos1	自定义	x16	未学习	未学习	正常	--
HBYD_WH_DDoS2	自定义	HBYD_WH_DDoS2;...	未学习	未学习	正常	--

图 6-54 基线学习状态

② 配置学习参数，如图 6-55 所示。



图 6-55　学习参数的配置

③ 基线学习任务启动后，系统每 5 分钟刷新一次学习结果。我们只有完成一个学习周期的学习，才能将学习结果应用到防御策略中。基线学习完成后，我们单击下面红框中的“详细”可以看到学习结果，如图 6-56 所示。

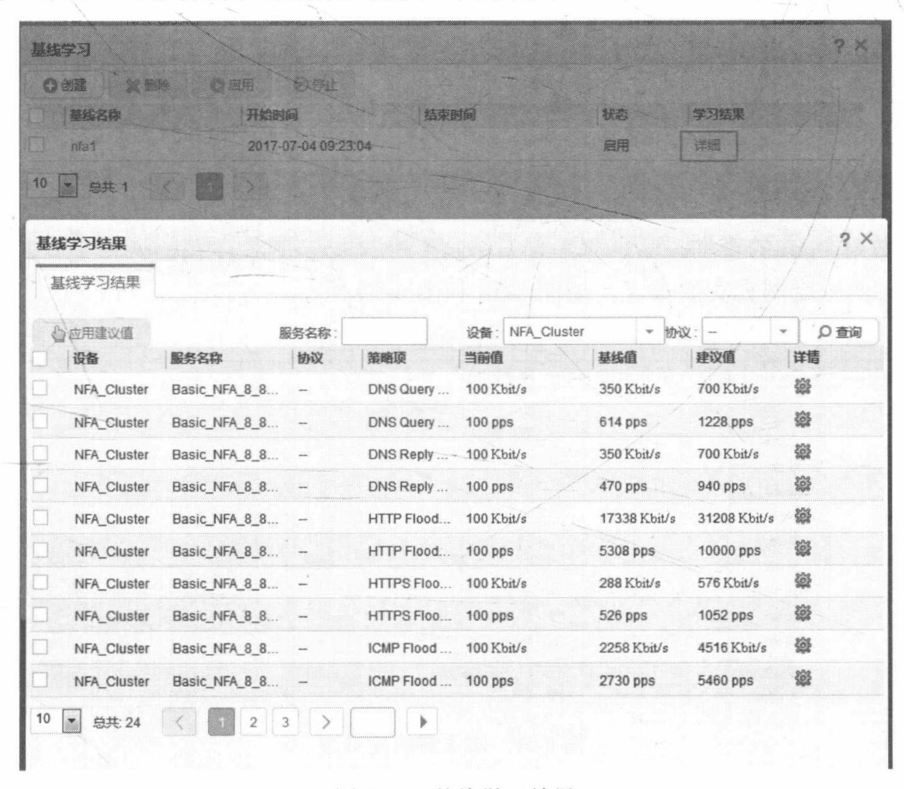


图 6-56　基线学习结果

当前值：它是指当前防御策略配置的阈值。

基线值：它是指基线学习学到的报文流量值。

建议值：它是对当前值和基线值经过一定计算得到的策略项的建议阈值。建议值下发到 Anti-DDoS 设备上后即变为当前值。

6.4.6 查看报表

ATIC 还提供了丰富的报表功能，用于展示流量模型。下面我们介绍一下报表的几个重要看点。

1. 正常流量与攻击流量的区分

Anti-DDoS 设备的流量对比报表中有三条曲线：入流量、出流量和攻击流量，如图 6-57 所示。



图 6-57 报表参数设置

从这简单的三条线我们能看出来什么呢？小图表隐含大内容。

报表支持不同粒度和维度的查询条件，IP 地址明确的情况下，设备可以针对指定的 IP 地址做单个 IP 的查询。

来看两张现网真实的报表，如图 6-58 和图 6-59 所示。

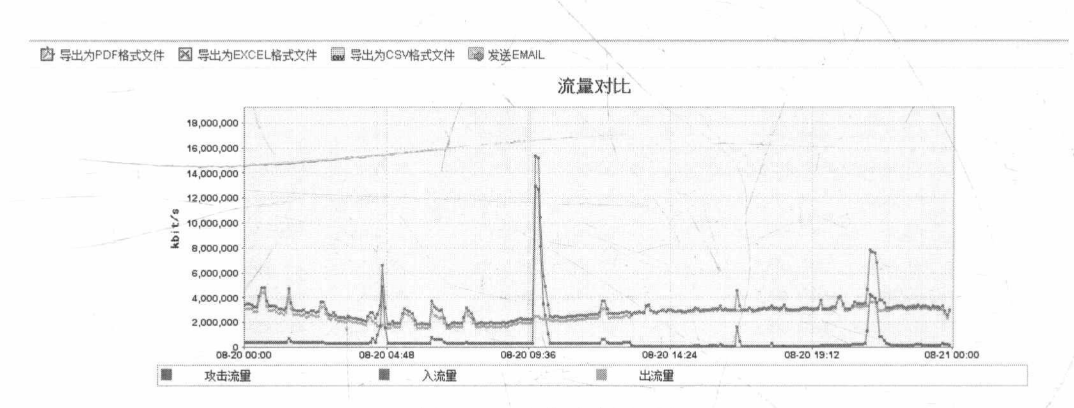


图 6-58 攻击时流量对比

正常的业务流量曲线的流量过度平滑，无明显的流量突发（电商活动抢购除外）。

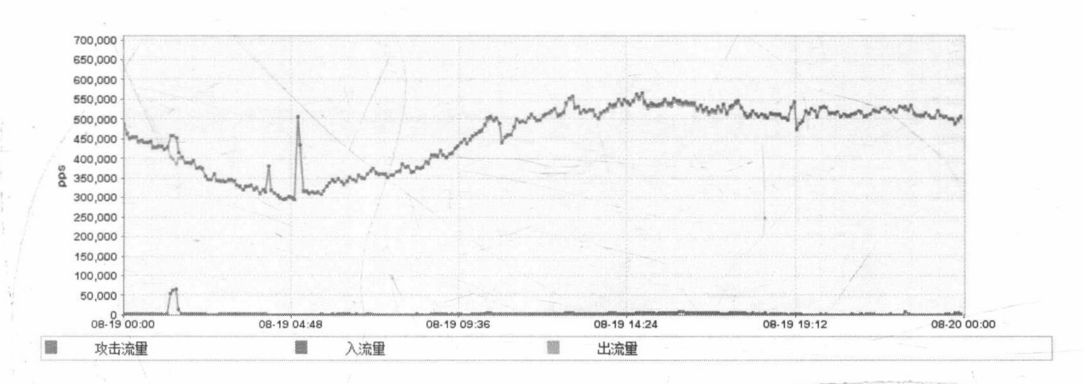


图 6-59 清洗后流量对比

① 图 6-58 中流量有明显的 3 次突发，有可能存在攻击。

② 图 6-59 中流量有一个明显的突发，但是突发的峰值不大，与全天的流量峰值持平，这个不一定是真的攻击。

2. 判定攻击的类型

回到查询条件，设备支持按照协议类型来查询流量曲线，如图 6-60～图 6-62 所示。

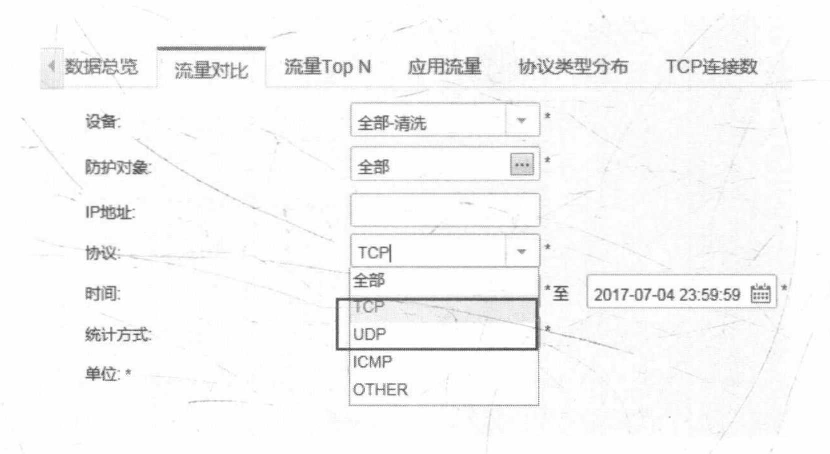


图 6-60 按照协议类型查询

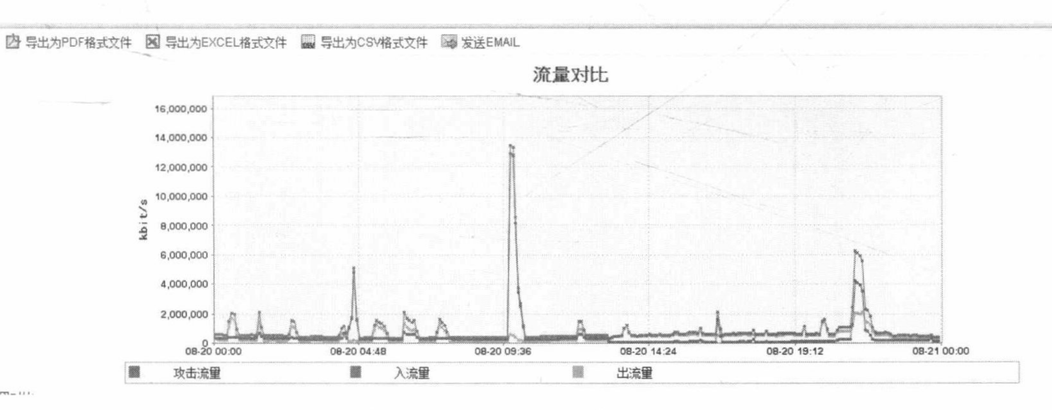


图 6-61 基于 UDP 的流量对比

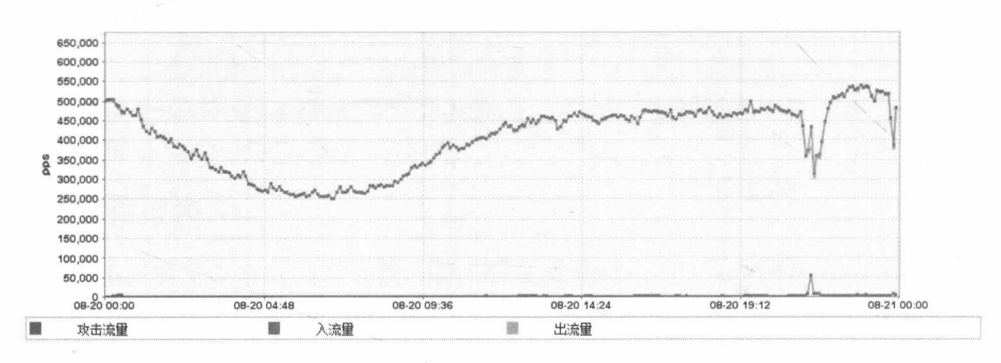


图 6-62 基于 TCP 的流量对比

从图 6-61 和图 6-62 可以看出，明显的 3 次流量突发都为 UDP 报文，即 UDP Flood 攻击。

3. 优化调整

如图 6-63 所示，防护效果主要显示流量曲线（第 2 条曲线）是否平滑，正常业务流量强度是否匹配。

① 出流量大，并且出流量仍然存在明显的突发，说明防护效果不好，可能存在漏防。

② 出流量小，并且出流量有明显的下降，可能存在误判。

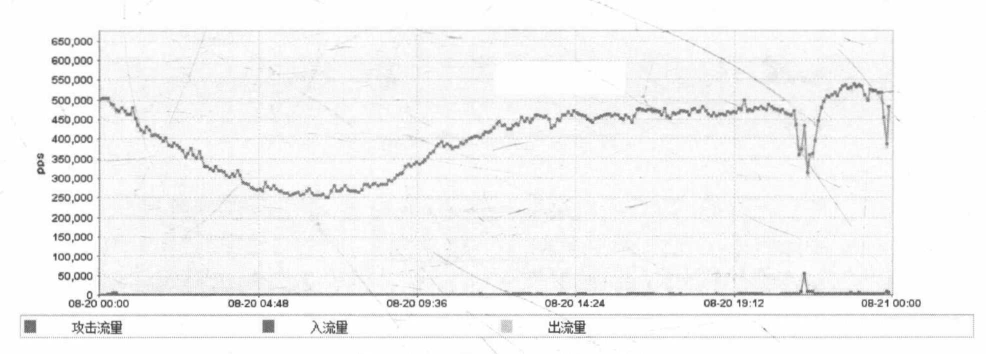
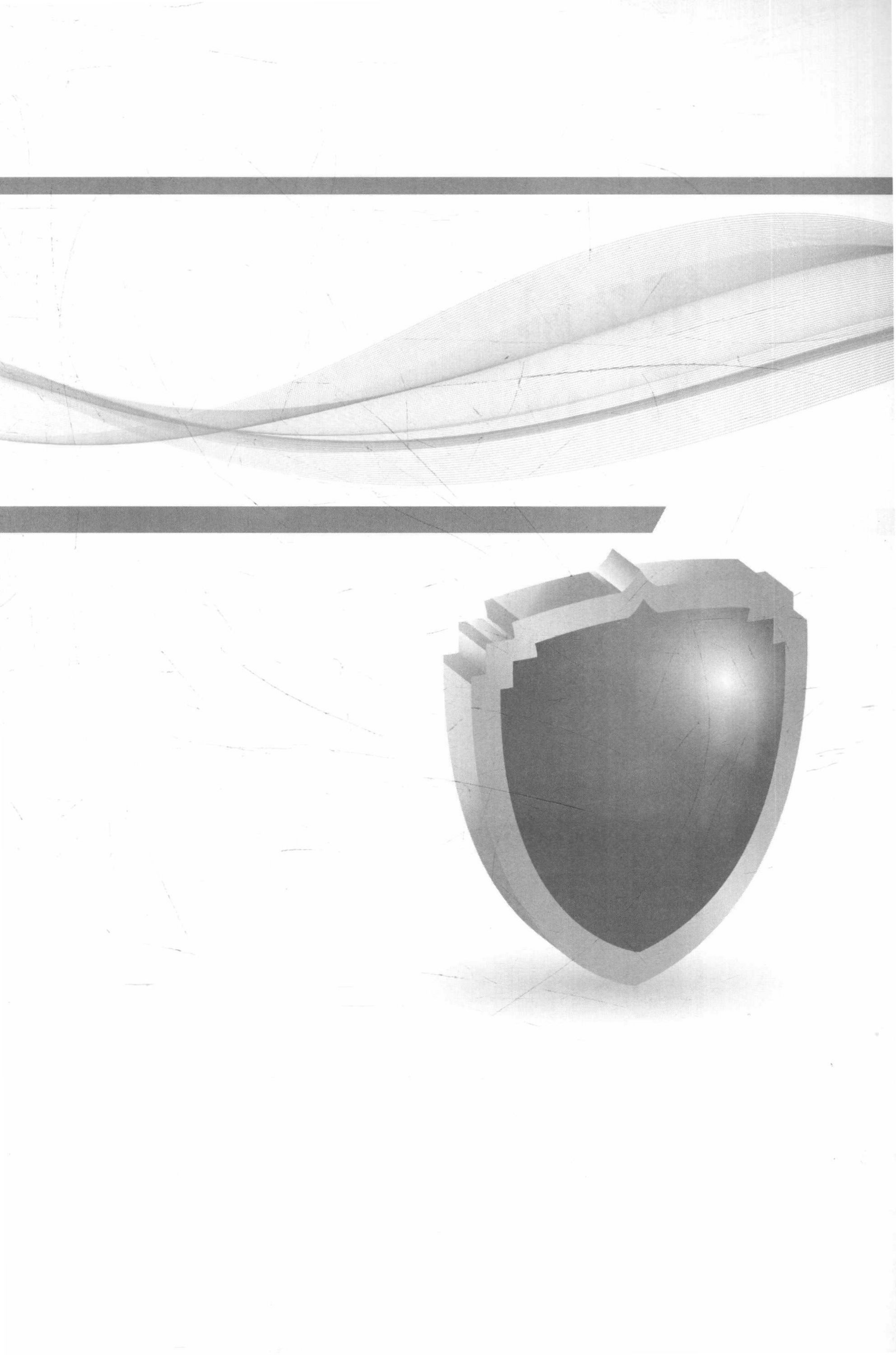
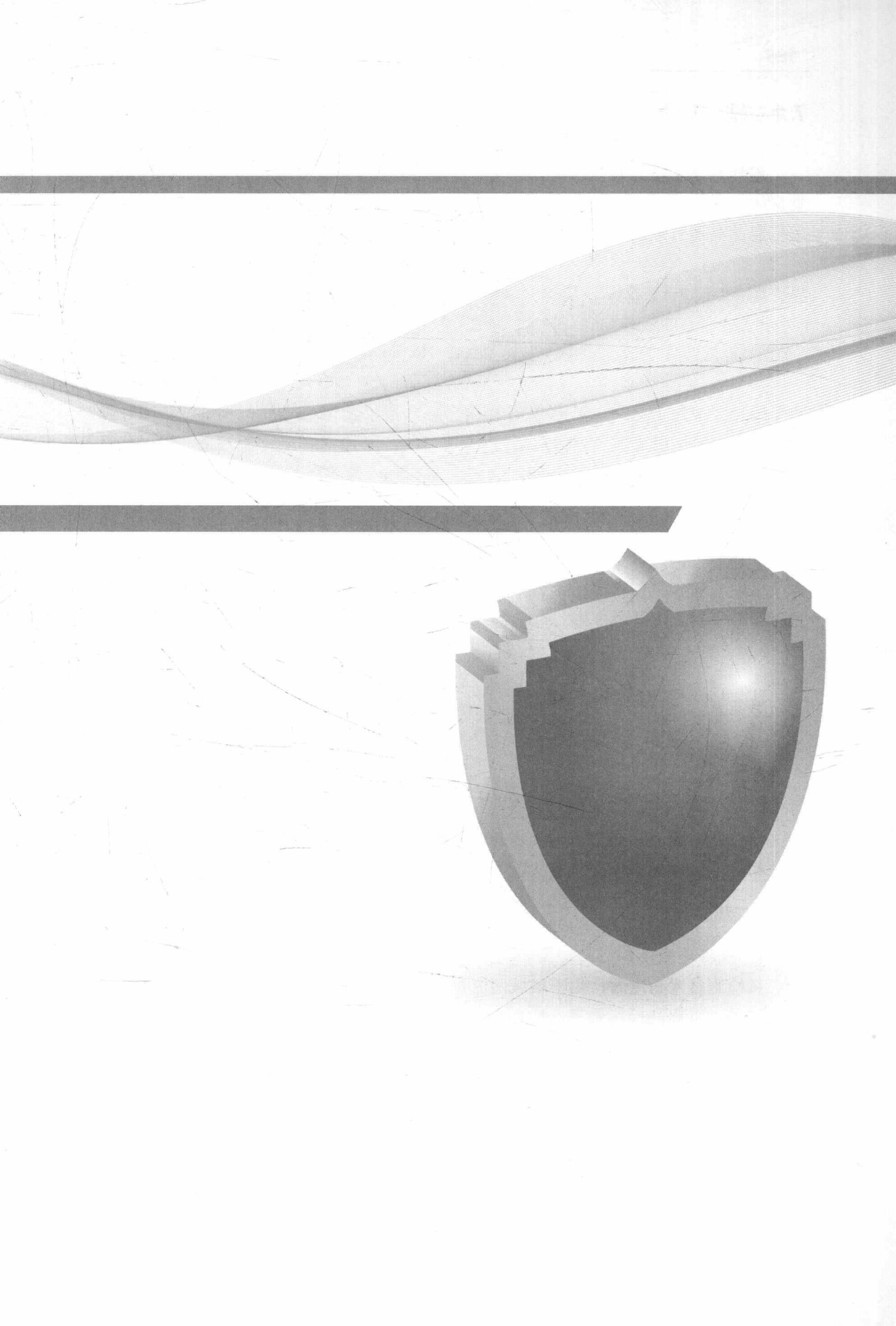


图 6-63 流量对比效果展示



第7篇 实　战



7.1 城域网防护

城域网是指在地域上覆盖一个城市，为城域多业务提供综合传送平台的网络。它主要应用于大中型城市地区，提供通用和公共的网络构架，以便数据、声音、图像和视频等信息的高速有效的传输，满足用户日新月异的互联网应用需求，如图 7-1 所示。

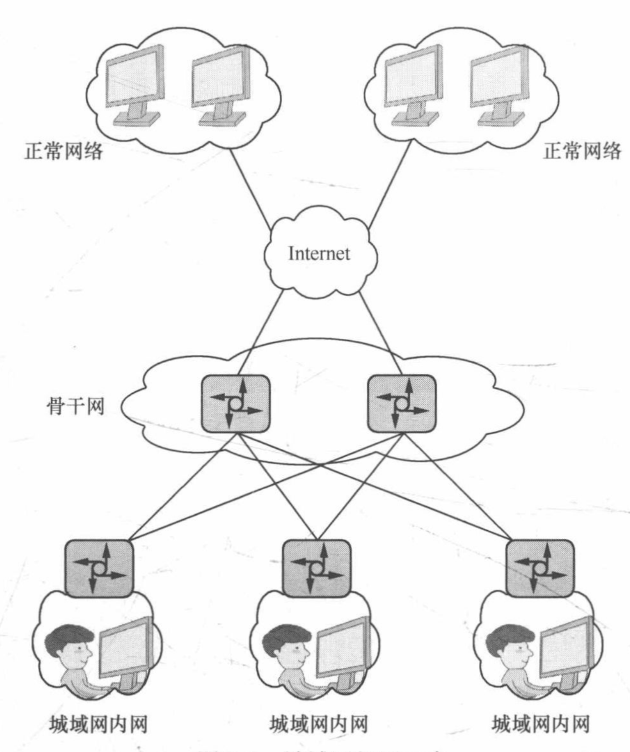


图 7-1 城域网组网示意

城域网中的流量很大、种类复杂，通常充斥着各式各样的攻击。针对城域网流量特点，相关人员规划城域网时可从以下几个方面考虑。

7.1.1 规划思路

1. 选择检测设备

从检测技术角度看，由于城域网流量非常大，我们可以采用逐流检测技术代替逐包检测技术，以提高检测效率。Netflow 设备属于抽样检测设备，可以应对城域网中的超大流量攻击，对性能要求不高。

从商务成本角度看，现网中已部署了很多的 Netflow 设备，这些 Netflow 设备可以直接与 Anti-DDoS 清洗设备联动，实现检测和清洗功能。用户通常无须单独购买检测设备，直接使用现网已存在的 Netflow 设备进行联动即可，成本较低。用户 Netflow 设备的价格也要比 Anti-DDoS 检测设备低，但在技术上也可满足工作的要求。

Anti-DDoS 设备不仅支持 Netflow 设备联动，也支持华为自研的 NFA 设备。

2. 清洗设备选择

由于城域网流量非常大，在发生攻击时，业务处理会消耗设备性能，所以建议用户将AntiDDoS8000作为清洗设备，其中，AntiDDoS8080设备或者AntiDDoS8160设备的业务处理能力很强。因为AntiDDoS8000是分布式插卡设备，所以可扩展性强。

对于具体的业务板卡和接口板卡的选配，用户要结合现网实际的带宽进行规划，并预留一定的清洗性能空间，从而应对大流量攻击场景。

3. 部署方式

在城域网场景中，我们通常采用AntiDDoS8000设备与Netflow设备进行联动，以从旁路部署组网。Netflow设备实时对现网流量进行检查，发现异常后，AntiDDoS8000设备会进行动态引流和清洗。这种动态引流的旁路部署组网只有在攻击发生时才会引流，所以可靠性最高。

4. 流量引导方式

城域网组网复杂，防护的IP地址多，通常采用BGP引流。回注方式主要依赖于客户的现网环境，通常使用MPLS LSP。运营商下行链路比较多，如果使用策略路由，需要依据不同的目的IP指定不同的下一跳。当目的IP比较分散时，配置复杂，其可使用MPLS LSP回注方式，在直连口开启MPLS LSP隧道。

5. 业务子卡规划

AntiDDoS8000是分布式设备，但设备是检测设备还是清洗设备取决于业务子卡的类型。在缺省情况下，AntiDDoS8000业务板的子卡不具备检测或清洗功能，用户需要通过命令指定某槽位业务子卡具有检测功能还是清洗功能。在本场景中，用户需要通过命令指定业务子卡具有清洗功能。

6. License控制

AntiDDoS8000业务板的子卡同时也会受License控制，命令制定后，要加载相匹配的License，才能生效。AntiDDoS8000设备的清洗License控制项见表7-1。

表7-1 AntiDDoS8000的清洗License控制项

资源项	适配的子卡	功能
清洗子卡-20	只能加载在ADS-SPC-20-00业务子卡上	激活License后，清洗功能可用
清洗子卡-40	只能加载在ADS-SPC-40-00业务子卡上	激活License后，清洗功能可用
清洗子卡-80	只能加载在ADS-SPC-80-00业务子卡上	激活License后，清洗功能可用

AntiDDoS8000设备支持使用主控板ESN和背板ESN申请License。主控板的ESN可以使用命令display esn进行查询，背板的ESN可以使用display esn all进行查询，显示的BackPlane为背板的ESN，也可以使用命令display license esn进行查询，我们推荐使用背板ESN申请License。因为主控板故障率比背板高，因此更换以后需要重新申请License，且其在双主控情况下需要使用两个ESN，当任何一个主控板出现故障时，License都要被更换。

在双主控情况下，主用主控板的ESN必须被同时提供。假如只使用主用主控板的ESN申请并激活License文件，那么设备还需要重新使用主用主控板和备用主控板的ESN去申请License文件，并取消已经激活的License文件，再激活新的License文件才可正常运行。

7. 接口规划

AntiDDoS8000 设备作为清洗设备需要具有一个引流口、一个回注口、一个与 ATIC 通信的管理口和一个日志口。

其中，引流口和回注口可以是两个不同的主接口，也可以是一个主接口下的两个子接口。

管理口和日志口，可以是同一个接口，也可以是不同的接口。主控板接口 GigabitEthernet0/0/0 可以作为与 ATIC 通信的管理接口，但不能作为向 ATIC 发送日志的接口。所以如果管理口和日志口用同一个接口的话，GigabitEthernet0/0/0 就不能作为接口。

ATIC 服务器只有 GE 接口，建议在接口板预留 1 个 GE 接口与 ATIC 互联。如果 AntiDDoS8000 设备上只有 10GE 接口，也可以使用中间网络设备进行 GE 接口与 10GE 接口的转换。

8. 防御策略

城域网中流量大，用户众多，一般以保证带宽、解决链路拥塞为防御目的。在部署时，工程师需要先甄别出需要重点保护的目的 IP 地址，加入自定义防护对象，并基于自定义防护对象配置相应的防御策略；对于不确定的要保护的目的 IP 地址，则用默认防护对象防御策略进行保护。工程师针对不同的防护对象应配置不同的防御策略。

如果运营商有运营上的需求，则可以创建自定义防护对象，将不同租户加入不同防护对象，为其配置差异化防御策略。

9. 安全策略规划

在缺省情况下，AntiDDoS8000 设备上的安全策略是关闭的，可以打开缺省包过滤。

10. ATIC

ATIC 由管理中心服务器和采集器两部分组成，并有两种部署方式。

① 集中式部署：ATIC 服务器和采集器同时安装在同一台物理服务器上。

② 分布式部署：ATIC 服务器和采集器分别安装在不同的物理服务器上，多台采集器可以共用一台 ATIC 服务器，一台 ATIC 服务器最多可管理 20 台采集器。

一台采集器可以处理大约 30 万个 IP 地址的 Anti-DDoS 业务日志，可以根据防护对象的 IP 地址个数来选择 ATIC 部署方式。设备旁路部署时，如果多台设备部署地比较分散，仍然建议配置多台采集器。

11. 路由规划

Netflow 设备、清洗设备、ATIC 三者之间要路由可达。

7.1.2 典型组网

如图 7-2 所示，清洗设备旁路部署在核心路由器 Router 1 上，对到达防护对象的流量进行清洗，清洗完成后，再将正常流量以 MPLS LSP 方式回注到原链路 Router 2，Router2 继续转发流量，最终将流量发送到防护对象。

清洗设备仅有一个接口与 Router 直连，主接口引流，子接口回注；在接口充足的情况下，其他主接口也可被用于回注。

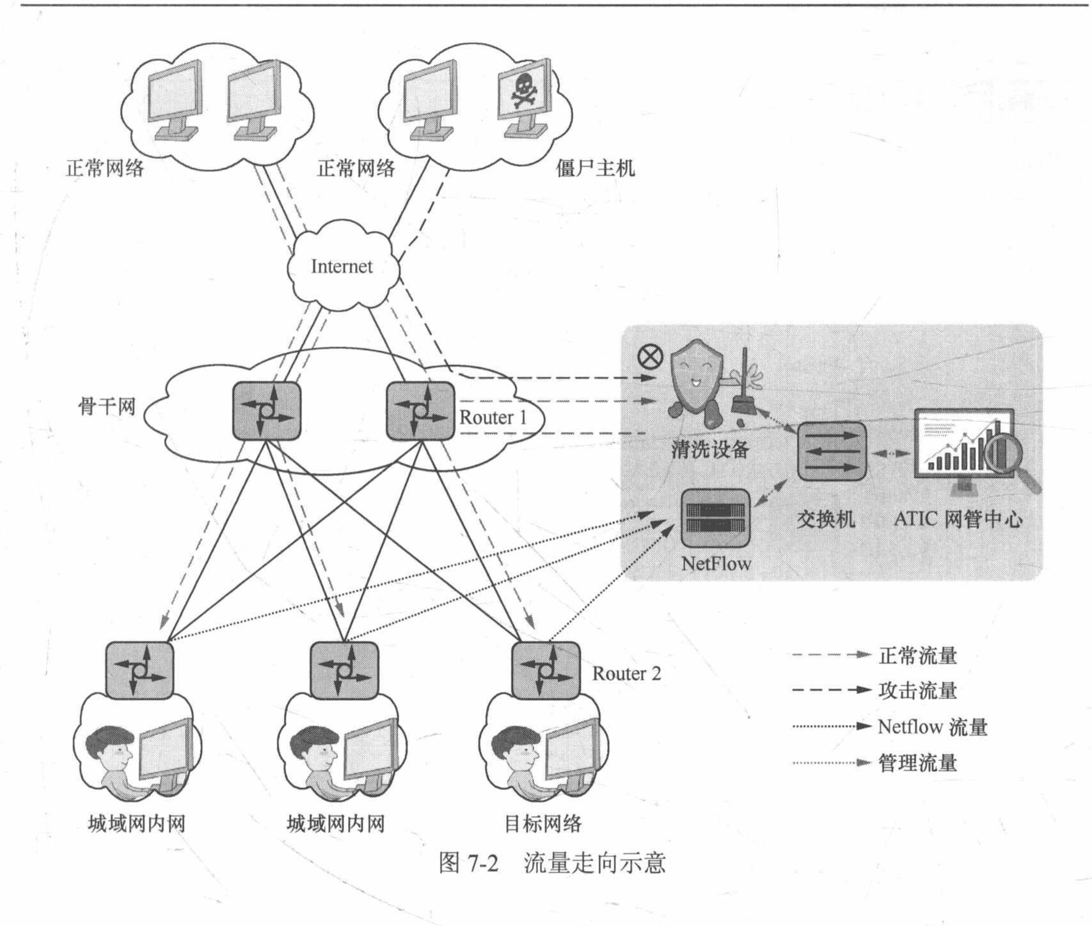


图 7-2　流量走向示意

7.1.3　数据规划

清洗设备和管理中心的 IP 地址规划，如表 7-2 和图 7-3 所示。

表 7-2　IP 地址规划表

设备名称	接口	IP 地址	说明
清洗设备	GE2/0/1	10.1.2.2/24	清洗口，即引流流量入接口，清洗设备对从该口进入的流量应用各种防御策略，对流量进行分析和清洗
	GE2/0/1.100	10.1.3.2/24	回注口，清洗后的正常流量通过此接口回注到原链路
	GE3/0/0	10.1.6.1/24	该设备和管理中心通信口，清洗设备将日志报文/抓包报文发送至管理中心的 Anti-DDoS 采集器，供 Anti-DDoS 采集器分析以及进行后续处理。 此接口 IP 地址与管理中心 IP 地址必须路由可达，本例中，此接口 IP 地址与管理中心在同一网段
	loopback 接口	2.2.2.2/32	用于 MPLS LSP 回注
管理中心	–	10.1.6.2/24	与清洗设备路由可达
Router 1	GE1/0/1	10.1.2.1/24	引流通道
	GE1/0/1.100	10.1.3.1/24	回注通道
	GE1/0/3	10.1.5.1/24	该设备和 Router 2 直连
	loopback 接口	5.5.5.5/32	用于 MPLS LSP 回注
Router 2	loopback 接口	3.3.3.3/32	用于 MPLS LSP 回注

（续表）

设备名称	接口	IP 地址	说明
Router 2	GE1/0/1	10.1.5.2/24	Router 2 Router1 直连
	GE1/0/3	10.1.7.2/24	Router 2 与 Netflow 设备路由可达
Netflow	Eth 0	10.1.7.1/24	Netflow 与 Router 2 直连
	Eth 1	10.1.6.3/24	Netflow 与管理中心通信口

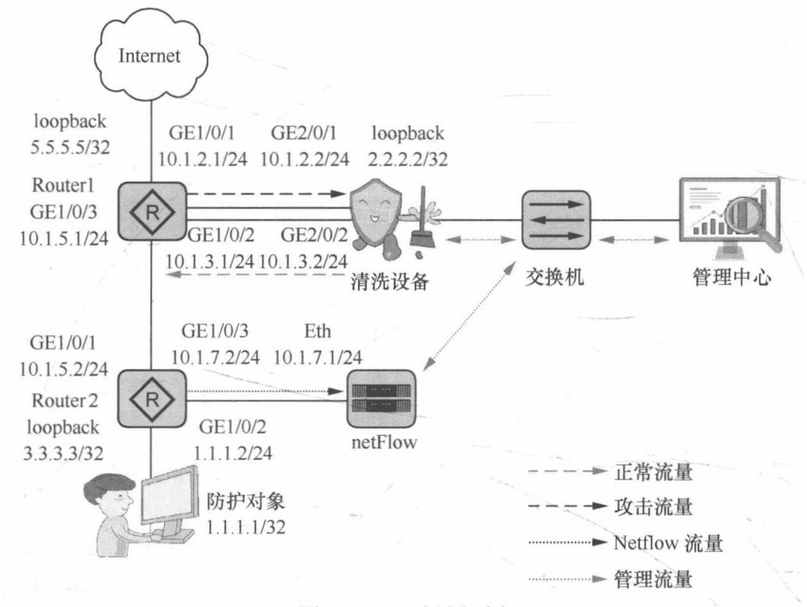


图 7-3 IP 地址规划

如果是威睿公司 Netflow 设备，必须为 2014 年 1 月 1 日以后的版本。

Router 1 的接口 GE1/0/1 与清洗设备的接口 GE2/0/1 之间的通道为引流通道。

Router 1 的接口 GE1/0/1.100 与清洗设备的接口 GE2/0/1.100 之间的通道为回注通道。

7.1.4 配置思路

1. 清洗设备的主要功能配置

① 加载 License。

② 指定业务子卡的类型。

③ 配置接口 IP 地址，接口加入安全区域，并打开域间缺省包过滤。

④ 更改缺省用户名和密码，并配置 Telnet 功能。

⑤ 配置 SNMP 功能，使管理中心可以获取清洗设备的状态。

⑥ 配置清洗口，并在清洗口开启流量统计功能。

⑦ 配置引流和回注功能。

⑧ 保存配置。

2. 管理中心的功能配置

① 第一次登录管理中心。

② 创建 Anti-DDoS 设备。

③ 配置相应的防御策略。

④ 保存配置。

另外，还要完成对接路由器的相关配置，本例给出的路由器配置仅作参考，在现网中，工程师应根据路由器的具体型号进行配置。

7.1.5 配置过程

1. 配置 ATIC

步骤 1 登录 ATIC。

在浏览器中输入管理中心 IP 地址，按“Enter”键。在登录界面输入用户名、密码和验证码。用户名为 admin，密码为 Admin@123，单击“登录”。第一次登录时界面会提示修改初始密码。

步骤 2 创建 Anti-DDoS 设备，将清洗设备添加到 ATIC，如图 7-4 所示。

创建设备 ? ×

设备信息

基本信息

设备名称： clean * IP地址： 10.1.6.1 *

类型： Anti-DDoS 日志源IP： 10.1.6.1

日志密码： ●●●●●●●●● *

Telnet参数

类型： STELNET

用户名： atic * 密码： ●●●●●●●●● *

公钥：

提示：
1.如果填写了公钥，使用STELNET、SFTP协议访问设备时对设备进行公钥认证。
2.为了保证数据传输的安全性，建议填写公钥。

SNMP参数

类型： SNMPv3 * 用户名： atic *

环境名称： 环境引擎ID：

授权认证协议： HMACSHA 授权认证密码： ●●●●●●●●● *

数据加密协议： AES128 数据加密密码： ●●●●●●●●● *

确定 取消

图 7-4 添加设备

① 选择“防御>网络配置>设备”。

② 单击 创建 。

• “IP 地址”指清洗设备管理口 IP 地址。

• “日志源 IP”指清洗设备的日志口 IP 地址。

• “日志密码”指上报日志的加密密钥。当成功创建设备后，ATIC 将密钥下发到 Anti-DDoS 设备上。

• STelnet 的参数和 SNMP 的参数配置要和清洗设备的配置必须保持完全一致，系统会进行校验。

③ 单击“确定”。Anti-DDoS 设备被成功添加到网元列表中。如果添加失败，工程师要检查 STelnet 的参数或者 SNMP 的参数是否与清洗设备的配置一致。

步骤 3 创建 Netflow 设备。如果有多台 Netflow 设备，则要添加多次创建，如图 7-5 所示。

① 选择“防御>网络配置>设备”。

② 单击 创建 。

③ 单击“确定”。Netflow 设备被成功添加到 ATIC 中。

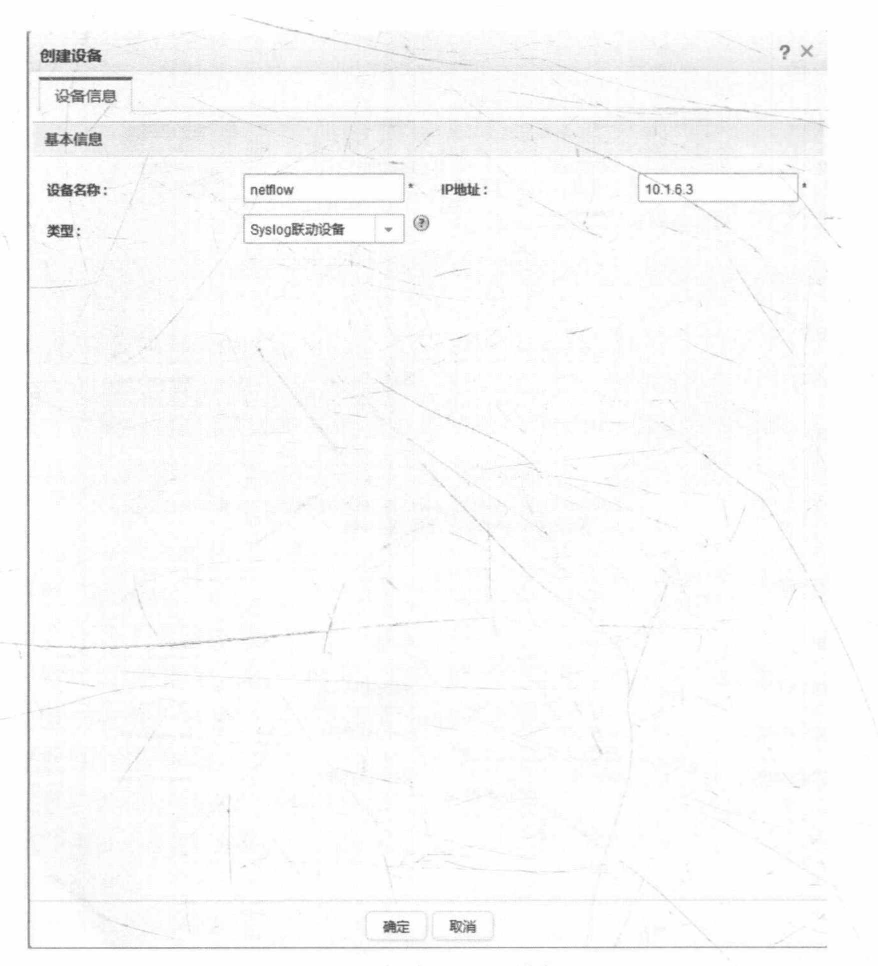


图 7-5 创建 netflow 设备

步骤 4　配置防御策略。

在配置防御策略时，工程师应先甄别出需要重点保护的目的 IP 地址，将其加入到自定义防护对象中，并基于自定义防护对象配置相应的防御策略；对于不确定的要保护的目的 IP 地址，则用默认防护对象防御策略对其进行保护。防御策略的配置要结合实际网络业务的特征进行，在城域网中，部署位置高，更多的是要保证链路的带宽。所以配置防御策略时，工程师可以考虑配置一些通用的防御策略。

① 选择“防御>策略配置>防护对象”，创建并单击默认防护对象对应的，如图 7-6 所示。

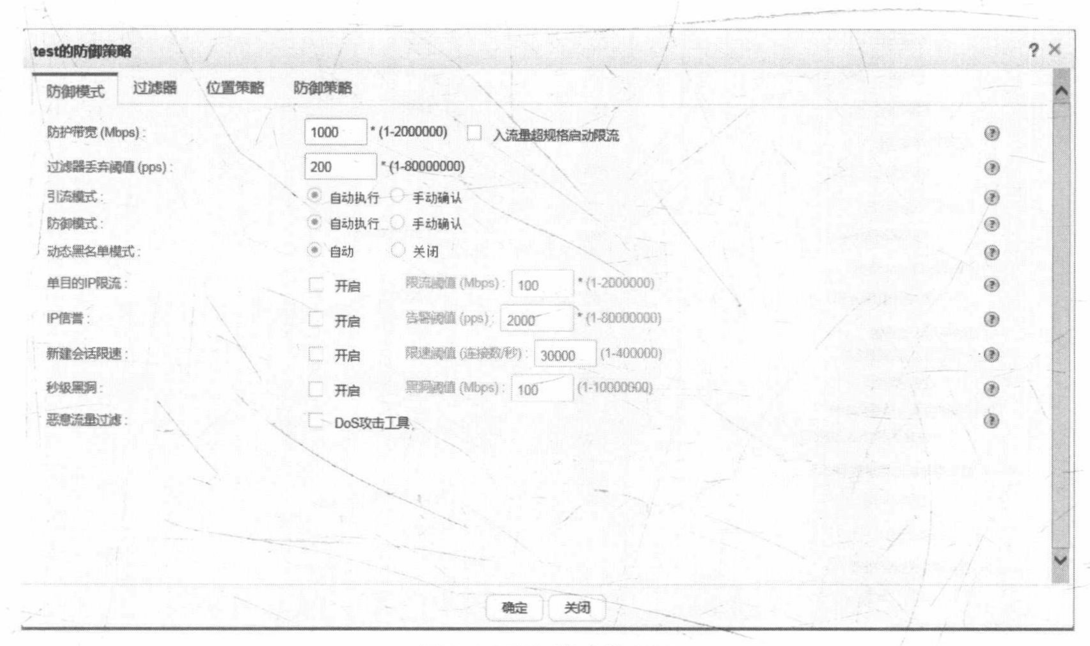


图 7-6　防御模式的配置

② 配置 TCP 通用防御策略。防御阈值可以根据基线学习的结果进行调整，如图 7-7 所示。

配置 ACK Flood 防御时，严格模式的防御效果优于宽松模式的防御效果。

- 在直路部署时，推荐使用严格模式。业务不会出现中断，防御效果要也优于宽松模式的防御效果。
- 在旁路部署时，建议使用宽松模式。如果工程师在旁路部署时使用严格模式，根据严格模式防御原理，业务在引流后，ACK 报文命中的会话必须是由 SYN 或 SYN-ACK 建立的，否则报文会被丢弃，会话重建后业务才会正常运行。

配置防御策略

TCP | UDP | ICMP | Other | DNS | SIP | HTTP | HTTPS | Top N学习 | 首包检查

配置项	值	范围
☑ 防御		
☑ TCP异常报文防御		
包速率阈值 (pps)：	1000	* (1-80000000)
☑ TCP基本防御		
☑ SYN Flood防御		
认证模式：	○ error-seq ◉ right-seq	
包速率阈值 (pps)：	2000	* (1-80000000)
☑ 源IP SYN报文比例异常限速		
SYN-Ratio比例阈值 (%)：	50	* (0-100)
检查周期 (秒)：	5	* (1-600)
SYN报文个数限速阈值 (个)：	200	* (0-80000000)
限速周期 (秒)：	10	* (1-600)
☑ ACK Flood防御		
包速率阈值 (pps)：	20000	* (1-80000000)
☑ TCP分片攻击防御		
包速率阈值 (pps)：	2000	* (1-80000000)
☑ FIN/RST Flood防御		
包速率阈值 (pps)：	500	* (1-80000000)
☑ TCP连接耗尽攻击防御		
目的IP地址并发连接数检查		
连接数阈值：	5000	* (1-80000000)
目的IP地址新建连接速率检查		
连接速率阈值 (连接数/秒)：	1000	* (1-10000000)
☐ 源IP地址新建连接速率检查		
连接数阈值：	200	* (1-80000000)
检查周期 (秒)：	5	* (1-60)
☐ 源IP地址连接数检查		
连接数阈值：	500	* (1-80000000)
☑ 异常会话检查		
异常连接数阈值：	30	* (1-255)
检查周期 (秒)：	15	* (1-240)
☑ 空连接检查		
每次连接最小报文数：	1	* (1-255)
检查周期 (秒)：	30	* (1-240)
☑ 重传会话检查		
重传报文阈值：	200	* (1-1023)
☑ Sockstress		
TCP窗口大小阈值 (字节)：	10	* (1-65535)

导入策略模板 | 导出策略模板 | 确定 | 取消

图 7-7 TCP 防御策略配置

③ 图 7-7 所示的配置在攻击时仅能告警，只有配置动态黑名单功能才能进行流量清洗，建议在应急的时候再开启动态黑名单功能，开启方法如图 7-8 所示。



图 7-8　开启动态黑名单

④ 配置 UDP 通用防御策略，如图 7-9 所示。

配置防御策略
TCP　UDP　ICMP　Other　DNS　SIP　HTTP　HTTPS　Top N学习　首包检查
阻断
限流
UDP限流
带宽阈值(Mbit/s): 500 * (1-2000000)
UDP分片限流
带宽阈值(Mbit/s): 50 * (1-2000000)
UDP新建会话限速
限速阈值(连接数/秒): 10000 (1-400000)
防御
导入策略模板　导出策略模板　确定　取消

图 7-9　UDP 防御策略配置

⑤ 配置 ICMP 通用防御策略，如图 7-10 所示。

⑥ 配置 Other 协议通用防御策略，如图 7-11 所示。

如果可以确认访问被保护的网络流量只有 TCP、UDP、ICMP 业务，不包含 IPSEC、GRE、IGMP 等其他协议，工程师可开启限流，防御效果会更好。



图 7-10 ICMP 防御策略的配置

如果存在 IPSEC、GRE、IGMP 等其他协议，则不能开启限流，否则会影响正常业务。

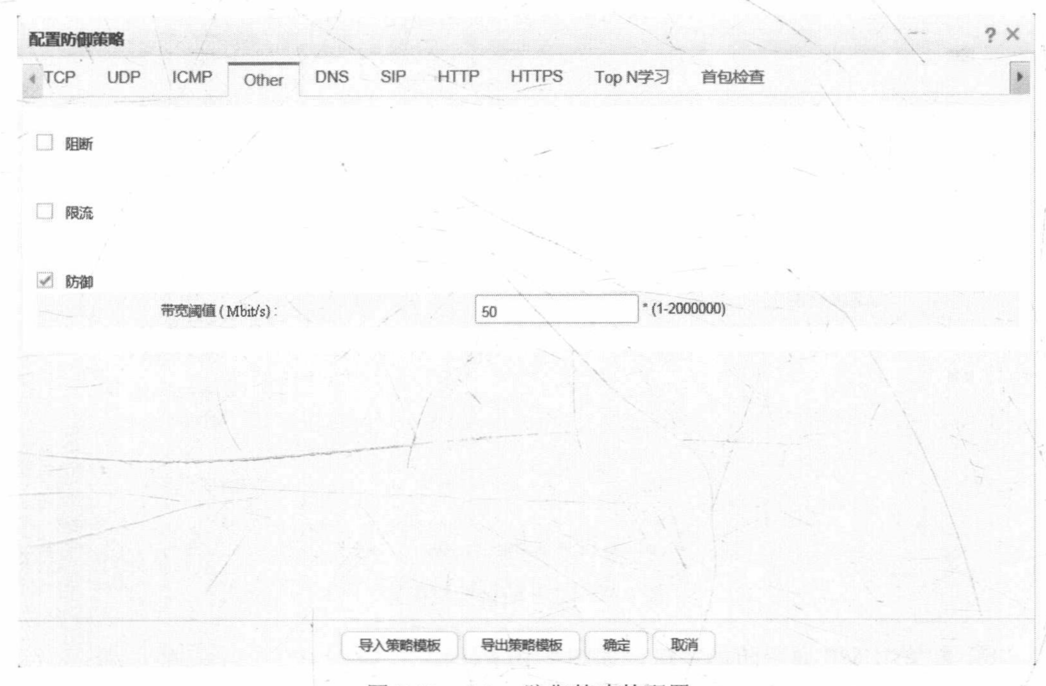


图 7-11 Other 防御策略的配置

⑦ 配置 DNS 协议通用防御策略，如图 7-12 所示。



图 7-12 DNS 防御策略配置

⑧ 配置 HTTP 通用防御策略，如图 7-13 所示。

多数用户的浏览器和 App 都有完整的 HTTP 协议栈，因此可以顺利通过"302 重定向"认证，当流量超过阈值触发防御后，用户感知不到认证过程，业务访问没有任何影响。但少数个别的 App 和程序可能使用不完整的 HTTP 协议栈，无法通过 HTTP "302 重定向"认证，导致业务受到影响，这个时候就需要关闭 HTTP 源认证防御，避免影响正常业务。



图 7-13 HTTP 防御策略的配置

⑨ 配置 HTTPS 通用防御策略，如图 7-14 所示。

图 7-14 HTTPS 防御策略的配置

⑩ 配置过滤器。对于不提供服务端口的攻击，通过配置过滤器进行阻断，否则将会影响防御效果。

我们单击“过滤器”，进入页签后，单击 关联过滤器，选中 ATIC 缺省提供的全部常用的过滤器模板，单击“确定”。

步骤 5 部署防御策略，并保存配置。

① 选择“防御 > 策略配置 > 防护对象”，选中防护对象前的复选框，单击部署。

② 单击“确定”，显示部署的进度提示，部署完成后，进度提示自动关闭。

③ 选择“防御 > 策略配置 > 设备全局配置”，选中 Anti-DDoS 设备前的复选框，单击 保存设备配置。

④ 单击“确定”，显示保存的进度提示，保存完成后，进度提示自动关闭。

2. 配置清洗设备

步骤 1 加载 License。

AntiDDoS8000 的清洗功能是受 License 控制的，所以用户在购买设备的同时，也要购买相应的 License。License 成功加载并激活是 AntiDDoS8000 清洗功能可用的前提条件之一。

License 文件后缀为*.dat，License 文件可以被重命名，但扩展名“.dat”不能被更改，否则系统将无法正常加载 License 文件。

激活License后，我们可以通过display license命令，查看License的信息。

```
<AntiDDoS> system-view
[AntiDDoS] license active lic_antiddos8000_20160530.dat
```

步骤2　指定业务板子卡使其具备清洗功能。

在缺省情况下，AntiDDoS8000 的业务子卡不具备清洗功能，需要通过命令指定。只有与子卡匹配的License处于激活状态时，在业务板底板注册成功后，AntiDDoS8000才可以执行下面的命令指定子卡类型。在子卡注册成功后，它才可以继续等其他配置。

```
[AntiDDoS] firewall ddos clean-spu slot 4 card 0
[AntiDDoS] firewall ddos clean-spu slot 4 card 1
[AntiDDoS] display ddos slot
Slot ID  Card ID  CPU Number  Config  Register  Status
------------------------------------------------------------------------------
4     0      0      clean  Registered  clean
4     1      2      clean  Registered  clean
------------------------------------------------------------------------------
```

步骤3　配置STelnet功能。

配置STelnet功能可帮助ATIC实现对清洗设备的管理，比如防御策略的下发、引流策略的下发等。ATIC和清洗设备的参数配置要保持完全一致。

```
[AntiDDoS] user-interface vty 0 4
[AntiDDoS-ui-vty0-4] authentication-mode aaa
[AntiDDoS-ui-vty0-4] user privilege level 3
[AntiDDoS-ui-vty0-4] protocol inbound ssh
[AntiDDoS-ui-vty0-4] quit
[AntiDDoS] aaa
[AntiDDoS-aaa] manager-user atic
[AntiDDoS-aaa-manager-user-atic] password
Enter Password:
Confirm Password:
[AntiDDoS-aaa-manager-user-atic] service-type ssh
[AntiDDoS-aaa-manager-user-atic] level 15
[AntiDDoS-aaa-manager-user-atic] quit
[AntiDDoS-aaa] quit
[AntiDDoS] rsa local-key-pair create
The key name will be: AntiDDoS_Host
The range of public key size is (512 ~ 2048).
NOTES: A key shorter than 1024 bits may cause security risks.
       The generation of a key longer than 512 bits may take several minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
...++++++++
..++++++++
.................................+++++++++
...........+++++++++
[AntiDDoS] stelnet server enable
[AntiDDoS] ssh user atic
[AntiDDoS] ssh user atic authentication-type password
[AntiDDoS] ssh user atic service-type stelnet
```

步骤4　配置接口IP地址，并将各接口加入相应的安全区域。

① 配置接口IP地址。

在缺省情况下，AntiDDoS8000接口开启了访问控制管理功能。管理接口（GE0/0/0）

下的 HTTP、HTTPS、Ping 权限都是放开的，不需要配置任何安全策略，就能通过管理口访问到设备。非管理口（包括逻辑接口，如 VLANIF、VT 接口、Tunnel 接口）下的 Telnet、Ping、SSH、SNMP 等权限都是关闭的。此时，即使放开了接口所在安全域到 local 的安全策略，非管理口也不能通过该接口访问设备。非管理口执行 **undo service-manage enable** 命令后，可以开启接口的 Telnet、Ping、SSH、SNMP 等功能。

```
[AntiDDoS] interface GigabitEthernet 2/0/1
[AntiDDoS-GigabitEthernet2/0/1] undo service-manage enable
[AntiDDoS-GigabitEthernet2/0/1] ip address 10.1.2.2 24
[AntiDDoS-GigabitEthernet2/0/1] quit
[AntiDDoS] interface GigabitEthernet 2/0/1.100
[AntiDDoS-GigabitEthernet2/0/1.100] undo service-manage enable
[AntiDDoS-GigabitEthernet2/0/1.100] ip address 10.1.3.2 24
[AntiDDoS-GigabitEthernet2/0/1.100] vlan-type dot1q 100
[AntiDDoS-GigabitEthernet2/0/1.100] quit
[AntiDDoS] interface GigabitEthernet 3/0/0
[AntiDDoS-GigabitEthernet3/0/0] undo service-manage enable
[AntiDDoS-GigabitEthernet3/0/0] ip address 10.1.6.1 24
[AntiDDoS-GigabitEthernet3/0/0] quit
```

② 加入安全区域。如果接口不加入安全区域，会导致业务不通。

```
[AntiDDoS] firewall zone trust
[AntiDDoS-zone-trust] add interface GigabitEthernet 2/0/1
[AntiDDoS-zone-trust] add interface GigabitEthernet 2/0/1.100
[AntiDDoS-zone-trust] add interface GigabitEthernet 3/0/0
[AntiDDoS-zone-trust] quit
```

步骤 5　打开域间缺省包过滤。

在缺省情况下，清洗设备的各域间安全策略是禁止通过的，我们需要将域间包过滤配置为允许，报文才能正常通过清洗设备。我们可不为清洗设备配置严格的安全策略，把所有安全策略打开即可。

```
[AntiDDoS] security-policy
[AntiDDoS-policy-security] default action permit
[AntiDDoS-policy-security] quit
```

步骤 6　配置 SNMP 功能。

同时在清洗设备和 ATIC 上配置 SNMP 功能，并保证配置参数一致，ATIC 便可以获取清洗设备的状态信息。

① 配置 ACL。ACL 仅允许 ATIC 通过 SNMP 访问清洗设备。

```
[AntiDDoS] acl 2998
[AntiDDoS-acl-basic-2998] rule permit source 10.1.6.2 0 description for snmp access
[AntiDDoS-acl-basic-2998] quit
```

② 将 ACL 与 SNMP 绑定。

```
[AntiDDoS] snmp-agent acl 2998
```

③ 配置 SNMP v3 功能。SNMPv3 方式安全性最高，推荐使用这种方式。

```
[AntiDDoS] snmp-agent sys-info version v3
[AntiDDoS] snmp-agent group v3 atic privacy acl 2998
[AntiDDoS] snmp-agent usm-user v3 atic
[AntiDDoS] snmp-agent usm-user v3 atic group atic
[AntiDDoS] snmp-agent usm-user v3 atic authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
```

```
Confirm Password:
[AntiDDoS] snmp-agent usm-user v3 atic privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
```

步骤 7　配置清洗口。

清洗口一般是指待清洗流量进入清洗设备的接口。在旁路部署的场景中，清洗口是引流流量的入口。从这个接口进入清洗设备的流量，要经过检测模块和清洗模块，所以我们需要在接口上指定接口类型并配置流量统计功能。

① 指定接口类型为清洗口。

清洗设备指定清洗口以后，从清洗口进来的报文才会被上送到清洗模块进行处理。

```
[AntiDDoS] interface GigabitEthernet 2/0/1
[AntiDDoS-GigabitEthernet2/0/1] anti-ddos clean enable
```

② 配置接口流量统计功能。

流量统计功能是清洗设备对流量进行清洗的前提条件，清洗口的流量统计功能一定要被开启，否则清洗功能不生效。在缺省情况下，接口流量统计功能处于关闭状态。

```
[AntiDDoS-GigabitEthernet2/0/1] anti-ddos flow-statistic enable
[AntiDDoS-GigabitEthernet2/0/1] quit
```

步骤 8　在清洗设备上，配置动态生成路由时使用的下一跳地址。

下一跳地址配置是与清洗设备回注接口直连的 Router 1 接口 GE1/0/1.100。当 netflow 设备检测到某个 IP 地址被攻击时，向 ATIC 通告攻击日志。ATIC 收到攻击日志后，会向清洗设备自动下发一条引流命令，这条引流命令和下面配置的下一跳地址命令相结合，会在清洗设备上生成一条 32 位 UNR 引流路由。这条引流路由会通过 BGP 发布到对端 Router 1 上。

这条引流路由要是路由器上优先级最高的路由，否则会导致引流失败。

```
<AntiDDoS> system-view
[AntiDDoS] firewall ddos bgp-next-hop 10.1.3.1
```

步骤 9　对生成的 32 位主机，UNR 路由进行 FIB 过滤。

清洗设备上生成 UNR 路由，并将其发布到对端路由器，实现引流，它还有回注的功能。如果不进行限制，由于 UNR 路由的优先级较高，当流量被引流到清洗设备上，完成清洗后，该流量可以通过清洗设备的这条 UNR 路由，再被送回到 Router 1 的接口 GE1/0/2 中。但是在很多场景中，回注链路比较多，流量不能只依赖 UNR 路由进行单链路回注，所以为了不让 UNR 路由影响回注，我们可设置让这条 UNR 路由不被下发到清洗设备的 FIB 表上，这样就不会影响回注。

本例使用的是 MPLS LSP 回注，所以我们要设置过滤掉这条 UNR 路由，不让其下发到 FIB 表。

```
[AntiDDoS] firewall ddos bgp-next-hop fib-filter
```

步骤 10　在清洗设备上配置 BGP 功能及团体属性。

清洗设备和 Router 1 之间建立 BGP 关系，Router 1 为引流路由器。当清洗设备生成 UNR 引流路由时，会通过 BGP 将其发布给 Router 1，实现引流功能，同时配置 BGP 团体属性，不向其他对等体发布匹配的路由。

```
[AntiDDoS] route-policy 1 permit node 1
[AntiDDoS-route-policy] apply community no-advertise
```

```
[AntiDDoS-route-policy] quit
[AntiDDoS] bgp 100
[AntiDDoS-bgp] peer 10.1.2.1 as-number 100
[AntiDDoS-bgp] import-route unr
[AntiDDoS-bgp] ipv4-family unicast
[AntiDDoS-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export
[AntiDDoS-bgp-af-ipv4] peer 10.1.2.1 advertise-community
[AntiDDoS-bgp-af-ipv4] quit
[AntiDDoS-bgp] quit
```

完成上述配置后，清洗设备上生成的 UNR 路由会被引入到 BGP 中，并通过 BGP 被发布到 Router 1。这样，当 Router 1 收到目的地址为 1.1.1.1/32 的流量时，通过查路由表，并根据最长掩码匹配原则，其会优先将流量从接口 GE1/0/1 转发至清洗设备。

步骤 11　配置清洗设备的 loopback 地址，该地址被用于配置 MPLS。

```
[AntiDDoS] interface loopback 1
[AntiDDoS-LoopBack1] ip address 2.2.2.2 32
[AntiDDoS-LoopBack1] quit
```

步骤 12　在清洗设备上配置 MPLS 功能，实现回注功能。

在清洗设备和 Router 2 之间建立 MPLS。回注的宗旨一方面是要把清洗后的流量回注到原链路中，然后将其送给防护对象；另一方面，就是要避开引流路由，防止路由环路发生。MPLS LSP 回注可以直接避开引流路由，将回注流量直接送到下行学习不到引流路由的路由器中，避免了路由环路问题的产生。

① 配置 MPLS 基本功能。

```
[AntiDDoS] mpls lsr-id 2.2.2.2
[AntiDDoS] mpls
[AntiDDoS-mpls] quit
[AntiDDoS] mpls ldp
[AntiDDoS-ldp] quit
[AntiDDoS] interface GigabitEthernet 2/0/1.100
[AntiDDoS-GigabitEthernet2/0/1.100] mpls
[AntiDDoS-GigabitEthernet2/0/1.100] mpls ldp
[AntiDDoS-GigabitEthernet2/0/1.100] quit
```

② 配置 LSP 的触发建立策略。

说明　配置 **lsp-trigger** 时，请根据实际需要建立隧道的 IP 进行配置。

```
[AntiDDoS] mpls
[AntiDDoS-mpls] lsp-trigger all
[AntiDDoS-mpls] quit
```

步骤 13　配置 OSPF，通告各接口所连网段的 IP 地址和 LSR ID 主机路由。

```
[AntiDDoS] ospf 1
[AntiDDoS-ospf-1] area 0
[AntiDDoS-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[AntiDDoS-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[AntiDDoS-ospf-1-area-0.0.0.0] quit
[AntiDDoS-ospf-1] quit
```

步骤 14　保存配置，要随时保存配置，以免丢失。

```
<AntiDDoS> save
```

3. Router 1 配置过程

下面以华为路由器 NE80E 为例，介绍 Router 1 的 BGP 和 MPLS 的配置过程。不同版本的路由器的配置也不同，请根据实际路由器版本进行配置，以下配置仅供参考。

步骤 1　配置 Router 1 接口的 IP 地址。

步骤 2　配置 Router 1 的 BGP 功能。

```
[Router1] bgp 100
[Router1-bgp] peer 10.1.2.2 as-number 100
[Router1-bgp] quit
```

步骤 3　配置 Router 1 的 loopback 地址。

```
[Router1] interface loopback 1
[Router1-LoopBack1] ip address 5.5.5.5 32
[Router1-LoopBack1] quit
```

步骤 4　配置 MPLS。

配置 MPLS 基本功能。

```
[Router1] mpls lsr-id 5.5.5.5
[Router1] mpls
[Router1-mpls] quit
[Router1] mpls ldp
[Router1-ldp] quit
[Router1] interface GigabitEthernet 1/0/1.100
[Router1-GigabitEthernet1/0/1.100] mpls
[Router1-GigabitEthernet1/0/1.100] mpls ldp
[Router1-GigabitEthernet1/0/1.100] quit
[Router1] interface GigabitEthernet 1/0/3
[Router1-GigabitEthernet1/0/3] mpls
[Router1-GigabitEthernet1/0/3] mpls ldp
[Router1-GigabitEthernet1/0/3] quit
```

步骤 5　配置 OSPF，通告各接口所连网段的 IP 地址和 LSR ID 主机路由。

```
[Router1] ospf 1
[Router1-ospf-1] area 0
[Router1-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[Router1-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255
[Router1-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[Router1-ospf-1-area-0.0.0.0] quit
[Router1-ospf-1] quit
```

4. Router 2 配置过程

下面以华为路由器 NE80E 为例，介绍 Router 2 的 MPLS 配置过程。

步骤 1　配置 Router 2 接口的 IP 地址。

步骤 2　配置 Router 2 的 loopback 地址。

```
[Router1] interface loopback 1
[Router1-LoopBack1] ip address 3.3.3.3 32
[Router1-LoopBack1] quit
```

步骤 3　配置 MPLS。

① 配置 MPLS 的基本功能。

```
[Router2] mpls lsr-id 3.3.3.3
[Router2] mpls
[Router2-mpls] quit
```

```
[Router2] mpls ldp
[Router2-ldp] quit
[Router2] interface GigabitEthernet 1/0/1
[Router2-GigabitEthernet1/0/1] mpls
[Router2-GigabitEthernet1/0/1] mpls ldp
[Router2-GigabitEthernet1/0/1] quit
```

② 配置 LSP 的触发建立策略。

```
[Router2] mpls
[Router2-mpls] lsp-trigger all
[Router2-mpls] quit
```

步骤 4　配置 OSPF，通告各接口所连网段的 IP 地址和 LSR ID 主机路由。

```
[Router2] ospf 1
[Router2-ospf-1] area 0
[Router2-ospf-1-area-0.0.0.0] network 10.1.5.0 0.0.0.255
[Router2-ospf-1-area-0.0.0.0] network 1.1.1.0 0.0.0.255
[Router2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[Router2-ospf-1-area-0.0.0.0] quit
[Router2-ospf-1] quit
```

步骤 5　Router 2 发送 Netflow 日志给威睿设备，路由器上的 Netflow 相关配置如下。

① 配置采样比，需要与威睿设备上配置相同。

```
[Router2] ip netstream sampler fix-packets 1000 inbound
```

② 配置 NetStream 输出报文的源地址。

```
[Router2] ip netstream export source 10.1.7.2
```

③ 配置 NetStream 输出的目的地址和端口号，即威睿设备地址。

```
[Router2] ip netstream export host 10.1.7.1 9900
```

④ 配置原始流 TCP-flag 的统计功能。

```
[Router2] ip netstream tcp-flag enable
```

⑤ 配置 NetStream 的老化时间。

```
[Router2] ip netstream timeout active 1
```

⑥ 指定接口板所在的 NetStream 板为 slot 1，NE40E 接口支持 NetStream 流量采集功能，无需购买专门的业务板。

```
[Router2] slot 1
[Router2-slot-1] ip netstream sampler to slot self
```

⑦ 接口板下对入方向的流量开启流量采集功能。

```
[Router2] interface GigabitEthernet1/0/1
[Router2-GigabitEthernet1/0/1] ip netstream inbound
```

5. 威睿设备配置

步骤 1　登录威睿设备。

① 第一次使用威睿服务器时使用串口登录并进行基本配置，PC 上串口的设置为（9 针串口线）。

Rate：9600 bit/s

Data bits：8

Parity：None

Stop bits：1

② 登录 GenieATM，默认用户名及密码均为“genie”。

③ 进入 Enable 模式。

```
ATM>enable
Password：default
```

Enable 模式默认密码为“default”。

④ 进入配置模式。

```
ATM# configure terminal
```

步骤 2　配置服务器 IP 地址和路由。

GenieATM 拥有 Ethernet0 和 Ethernet1 两个以太电接口。路由可达的情况下，服务器访问和流量采集可以共用一个端口。如果采用两个不同网口，有一个值得注意的地方是系统的默认路由只能设定在 E0 口上，另外一个口的路由需要手工静态设定。

```
ATM (config)# interface Ethernet 0
ATM (config-if)# ip address 10.1.7.1 255.255.255.0
ATM (config-if)# exit
ATM (config)# interface Ethernet 1
ATM (config-if)# ip address 10.1.6.3 255.255.255.0
ATM (config-if)# exit
```

步骤 3　配置 log 服务器。

配置 log 服务器，使 GenieATM 可以成功发送攻击日志到 ATIC 服务器。此配置为 AntiDDoS 与 GenieATM 联动的关键配置。

```
ATM# logging on
ATM# logging buffer-size 4096
ATM# logging source-interface ethernet 0      //日志发送源接口
ATM# logging server 10.1.6.2      //ATIC 服务器地址
```

步骤 4　保存配置并重启服务器。

① 保存配置。

```
ATM# write config
```

② 重启 GenieATM。

```
ATM# reload now
```

6. 配置 Genie 管理服务器

步骤 1　登录 Genie 管理服务器。

步骤 2　添加流量采集设备，如图 7-15 所示。

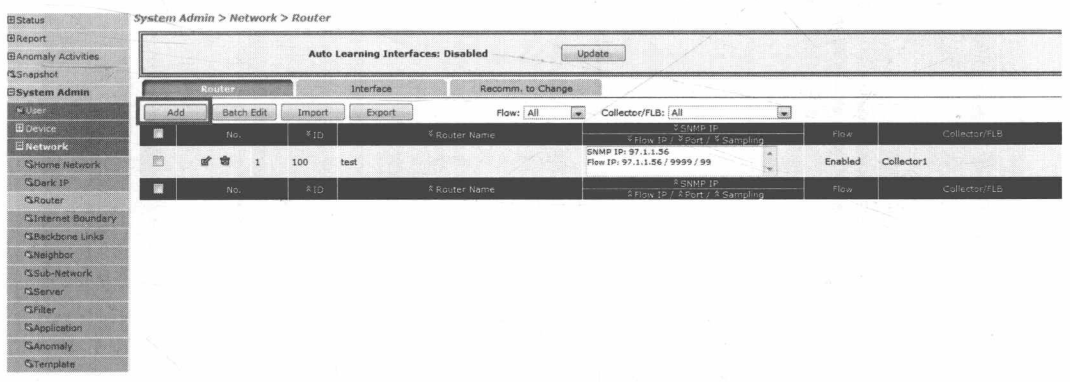


图 7-15　添加流量的采集设备

步骤 3　点击“新增”。添加流量采集路由器的 SNMP IP 地址、读团体字符串、SNMP 版本号；填写 Flow 输出设备的 IP 地址和端口号，即流量采集路由器输出 Netflow 接口的地址和端口号，采样率需要与路由器的相同，如图 7-16 所示。

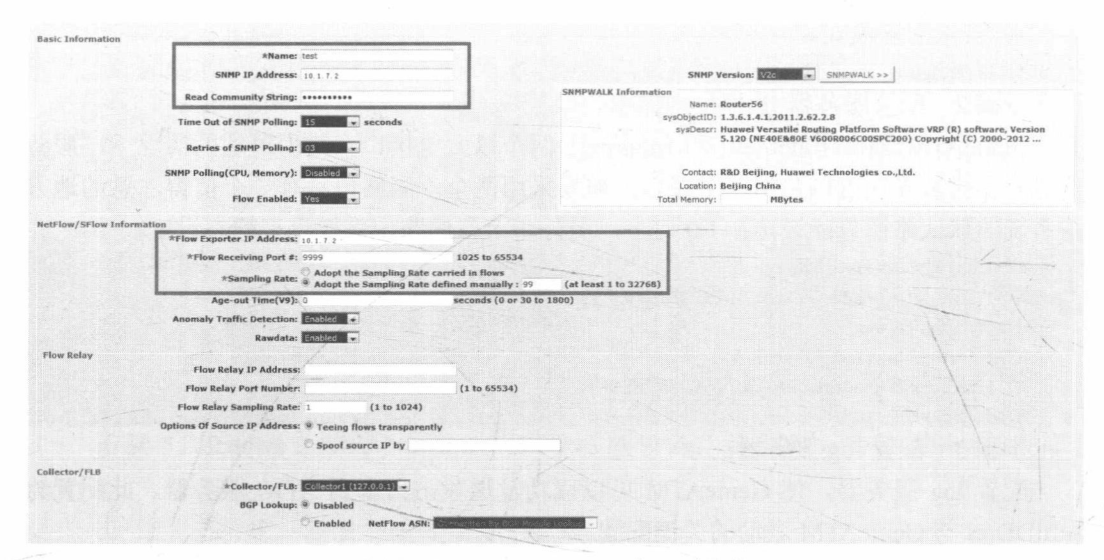


图 7-16　流量采集路由器的配置参数

步骤 4　“系统管理”>“网络>本域网络”，自定义监控的目的 IP 地址，如图 7-17 所示。

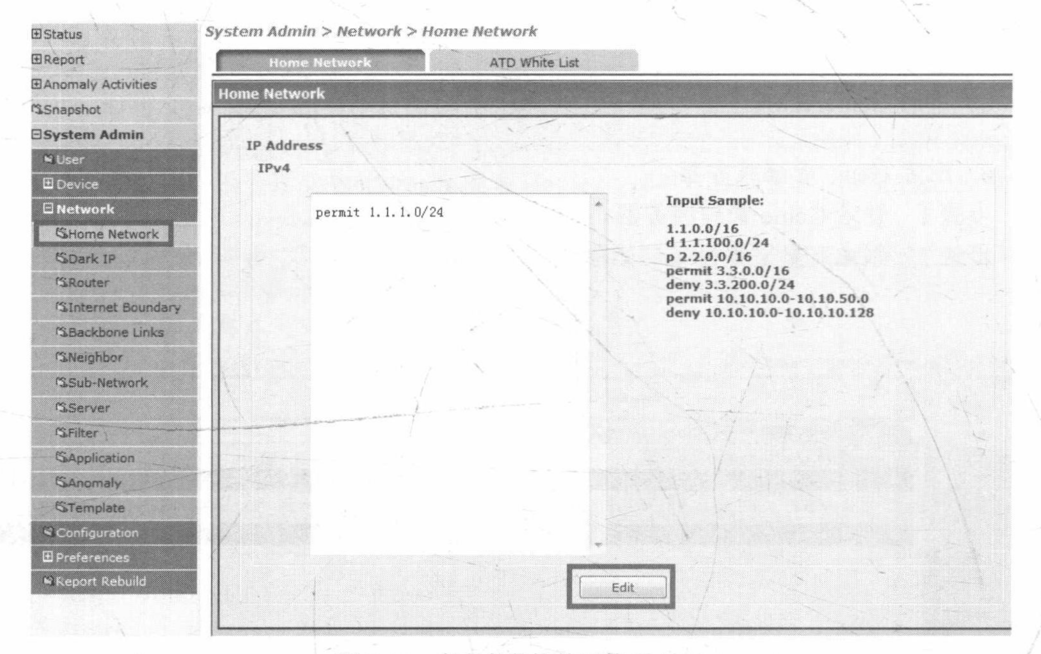


图 7-17　自定义监控的目的 IP 地址

点击“编辑”，添加监控的 IP 地址。

步骤 5　威睿服务器预定义异常流量的攻击，如图 7-18 所示。

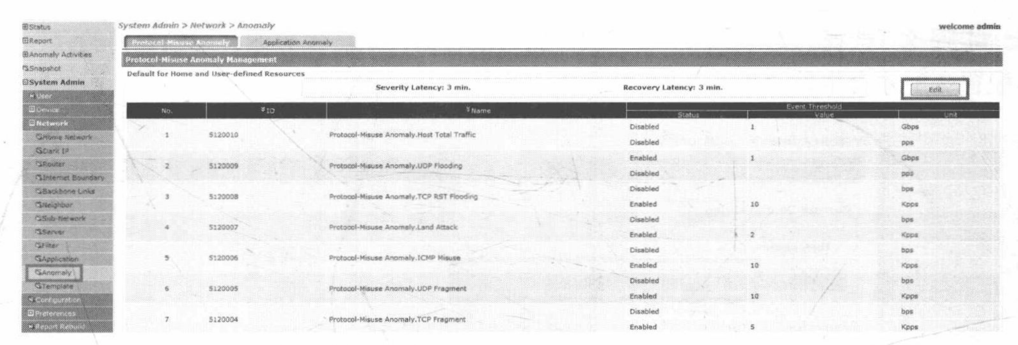


图 7-18　预定义异常流量的攻击

点击“编辑”按钮可以修改预定义攻击的状态、阈值和单位。

步骤 6　威睿服务器自定义异常流量的攻击，如图 7-19 所示。

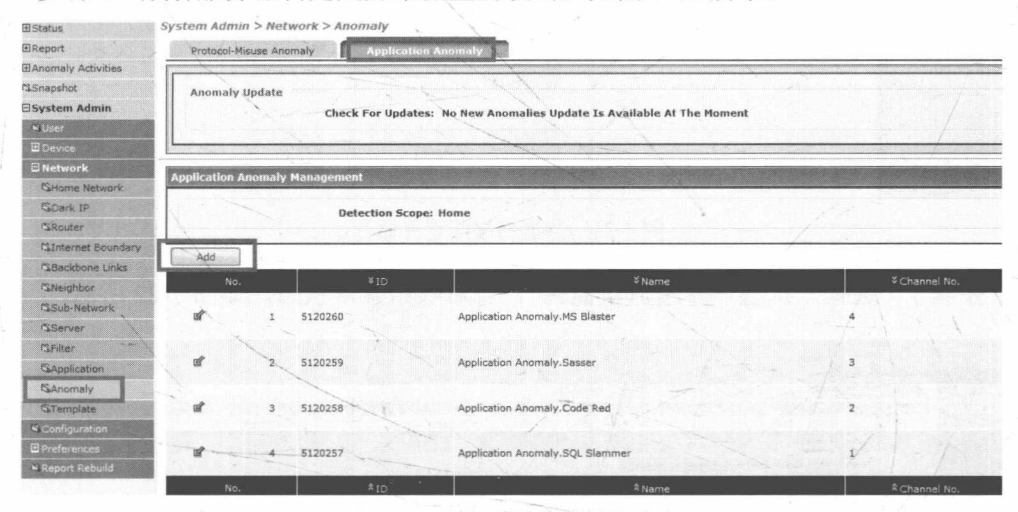


图 7-19　自定义异常流量的攻击

步骤 7　点击“新增”，增加自定义攻击类型，如图 7-20 所示。

Protocol-Misuse Anomaly　Application Anomaly

Add Application Anomaly

Application Anomaly

*ID: 5120356

*Application Name:Channel Name: Application Anomaly : SYN-ACK Flood

*Application No.:Channel No.: 20001 : 100

*Status: Enabled

Remarks:

*Attack Type: DDoS

Characteristics

Number of Packets Per Flow:

Number of Bytes per Flow:

Number of Bytes per Packet:

TCP Flag: URG ACK PSH RST SYN FIN

TOS Value: 8 7 6 5 4 3 2 1

Protocol: IP/0　ICMP Message Type:　Code:

Port: Src. or Dst.

Dark IP: Source IP for Incoming Traffic; Destination IP for Outgoing Traffic

Prefix: Src.

IPv4

Baseline

Event Threshold　Unit　Severity Latency　Recovery Latency

图 7-20　自定义攻击类型

步骤 8　选择“系统管理 > 配置”，输入描述后，点击“分派网络配置并储存”，这样配置变更才会生效，如图 7-21 所示。

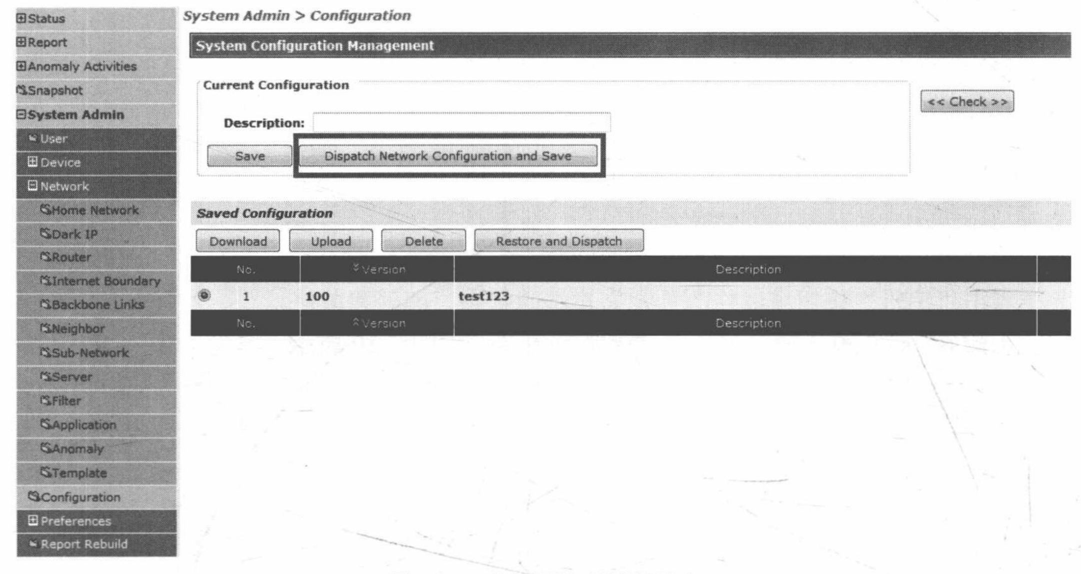


图 7-21　分派网络配置并储存

步骤 9　选择“状态 > 异常流量监控”，查看攻击异常状态，如图 7-22 所示。

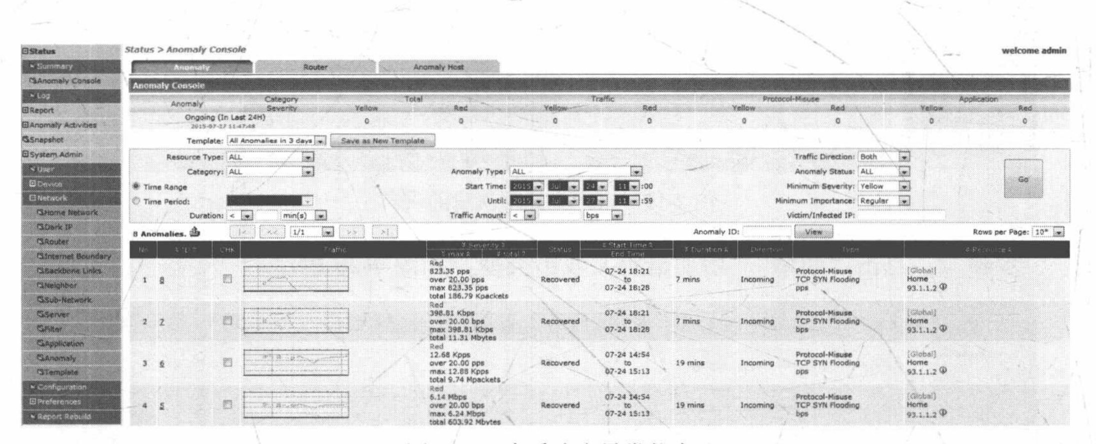


图 7-22　查看攻击异常状态

7.2　小型数据中心防护

数据中心是网络基础资源的一部分，为互联网内容提供商、企业、媒体和各类网站提供大规模、高质量、安全可靠的数据传输服务和高速接入服务。小型、超小型数据中心主要是接入层机房，比如银行、证券的网点机房，政府各部门服务窗口等。图 7-23 所示的网络相对简单，业务也比较固定，防护目标也很明确。近年来，外部互联网对数据

中心发起的 DDoS 攻击越来越多，其中包括重要用户服务器遭受攻击，数据中心链路带宽被占用，视频、游戏、网游等业务遭受到应用层攻击等。

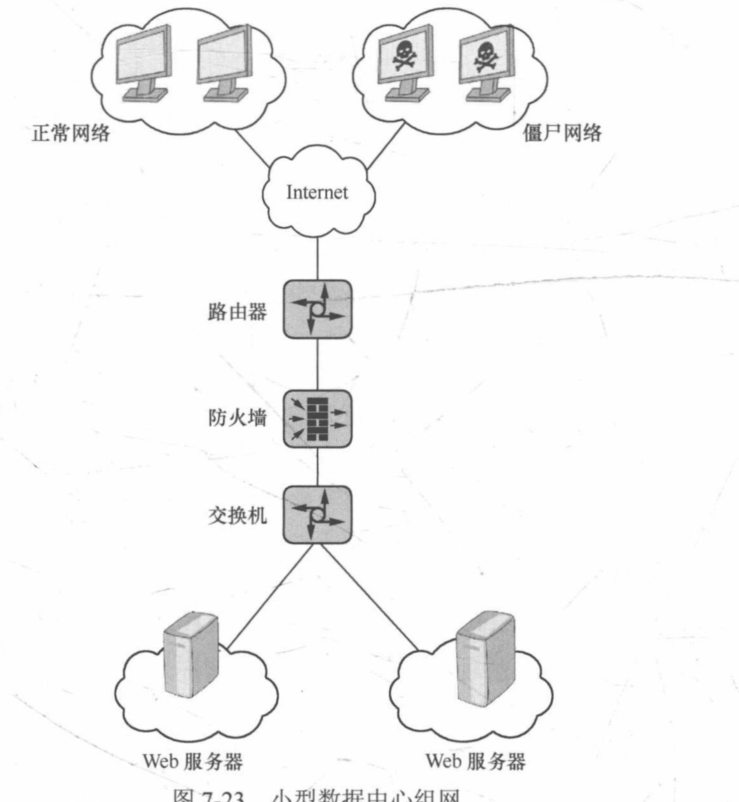


图 7-23　小型数据中心组网

为了保障数据中心业务服务器的网络免受 DDoS 攻击，保证正常业务不间断，工程师规划网络时应从以下几个方面考虑。

7.2.1　规划思路

1. 设备选择

数据中心有存储各种重要业务信息的服务器，这些服务器承载了现网中的各种业务，服务器一旦受到攻击，会直接导致部分网络瘫痪，影响正常业务的运行。所以数据中心的检测和清洗精准度非常重要。华为 AntiDDoS8000 设备采用的是逐包检测技术。相比于逐流检测，逐包检测更精细，工程师也可同时为不同的业务配置差异化防御策略。逐包检测的防御更精准，推荐使用。

2. 部署方式

旁路部署方式不改变原有网络的拓扑结构，同时还可以保证链路的可靠性。

除了“检测+清洗”联动旁路部署的方式外，AntiDDoS8000 设备还支持混插模式。混插模式是一台 AntiDDoS8000 设备同时插检测业务板和清洗业务板，该方式集成“检测设备”和“清洗设备”，效果上和“检测+清洗”联动是一样的，也是检测模块和清洗模块分离，支持实时检测和动态清洗。

从商务成本方面考虑，AntiDDoS8000 设备的混插模式的成本低于同时部署 1 台 AntiDDoS8000 检测设备和 1 台 AntiDDoS8000 清洗设备的成本，用户购买一台机柜即可混插不同类型的业务板。

3. 流量引导方式

数据中心组网不会很复杂，回注链路也不会太多，建议采用 BGP 旁路引流+策略路由回注方式引导流量。BGP 引流可以实现动态引流，策略路由回注配置简单。

Anti-DDoS 设备既支持静态引流，也支持动态引流。静态引流清洗是指不管是否发生攻击，Anti-DDoS 设备都将所有流量引导到清洗设备中，再由清洗设备转发流量。当发生攻击时，清洗过程会非常消耗清洗设备的性能。一旦清洗设备性能达到瓶颈状态，就会影响流量的转发。如果此时 Anti-DDoS 设备还需要转发其他用户的流量，只要设备性能稍有问题，没有遭受攻击的用户业务也会受影响。相比于静态引流方式，动态引流可靠性更高。使用动态引流，没有发生攻击时，流量并不会经过清洗设备；只有攻击发生后，清洗设备才会将去往被攻击用户的流量引流到设备上进行清洗，其他未受到攻击的用户的流量不会被引流，也不经过清洗设备。因此，即使清洗设备流量很大也不会影响其他用户。

4. 业务子卡规划

AntiDDoS8000 是分布式设备，设备是检测设备还是清洗设备取决于业务子卡的类型。在缺省情况下，AntiDDoS8000 业务板的子卡不具有检测或清洗功能，用户需要通过命令指定某槽位业务子卡的功能是检测功能或者清洗功能。

5. License 控制

AntiDDoS8000 业务板的子卡同时也受 License 控制，命令制订后，要加载相匹配的 License，才能生效。AntiDDoS8000 的检测和清洗 License 控制项见表 7-3。

表 7-3　AntiDDoS8000 的检测和清洗 License 控制项

资源项	适配的子卡	功能
检测子卡-20	只能加载在 ADS-SPC-20-00 业务子卡上	激活 License 后，检测功能可用
检测子卡-40	只能加载在 ADS-SPC-40-00 业务子卡上	激活 License 后，检测功能可用
检测子卡-80	只能加载在 ADS-SPC-80-00 业务子卡上	激活 License 后，检测功能可用
清洗子卡-20	只能加载在 ADS-SPC-20-00 业务子卡上	激活 License 后，清洗功能可用
清洗子卡-40	只能加载在 ADS-SPC-40-00 业务子卡上	激活 License 后，清洗功能可用
清洗子卡-80	只能加载在 ADS-SPC-80-00 业务子卡上	激活 License 后，清洗功能可用

AntiDDoS8000 支持使用主控板 ESN 和背板 ESN 申请 License。主控板的 ESN 可以通过命令 display esn 查询，背板的 ESN 可以通过命令 display esn all 查询，显示的 BackPlane 为背板的 ESN，也可以通过命令 display license esn 查询。推荐使用背板 ESN 申请 License。因为主控板故障率比背板高，更换以后需要重新申请 License，双主控情况下需要使用两个 ESN，任何一个主控板故障都要更换 license。

在双主控情况下，AntiDDoS8000 设备必须同时提供主备主控板的 ESN。假如只使用主用主控板的 ESN 申请并激活 License 文件，需要重新使用主用主控板和备用主控板的 ESN 去申请 License 文件，取消已经激活的 License 文件，再激活新的 License 文件即可正常使用。

6. 接口规划

工程师规划混插设备时需要规划一个检测口、一个清洗口（引流口）、一个回注口、一个与 ATIC 通信的管理口和一个日志口。其中，引流口和回注口可以是两个不同的主接口，也可以是一个主接口下的两个子接口。

管理口和日志口可以是同一个接口，也可以是不同的接口。主控板接口 GigabitEthernet0/0/0 可以作为与 ATIC 通信的管理接口，但不能作为向 ATIC 发送日志的接口。如果管理口和日志口用同一个接口的话，就不能用 GigabitEthernet0/0/0。

ATIC 服务器只有 GE 接口，建议在接口板预留 1 个 GE 接口与 ATIC 互连。如果 AntiDDoS8000 设备上只有 10GE 接口，也可以使用中间网络设备进行 GE 接口与 10GE 接口的转换。

7. 防御策略

首先明确设备要防护的目标 IP，针对目标建立防护对象，然后配置相应的防护策略。对于其他不明确的目标，配置默认防护对象的防御策略来对其进行防御。

例如：IDC 网络中有 3 台 Web 服务器、2 台 DNS 服务器、5 台游戏服务器，工程师应为不同的服务器配置不同的防御策略，为 Web 服务器重点配置 HTTP 类的防御策略，为 DNS 服务器重点配置 DNS 类的防御策略，为游戏服务器重点配置 UDP/TCP 类的防御策略等。

如果我们为每一个服务器建立一个防护对象，则我们需要建立 10 个防护对象，配置起来比较麻烦。如果同一类型的服务器业务基本相同，则可以只配置三个防护对象，即针对 Web 服务器、DNS 服务器和游戏服务器的 3 个防护对象，然后，在每一个防护对象中把多个服务器 IP 地址添加进来（每个防护对象可以配置多个 IP 或者网段），再配置相应的防御策略，这样每一类服务器只需要配置一次策略即可。

配置完成后，完成了对重点目标的防护，也可以对 IDC 中其他的网络资源使用默认防护对象的防御策略进行防御。

8. 安全策略规划

在缺省情况下，AntiDDoS8000 设备上的安全策略是关闭的，但我们可以打开缺省包过滤。

9. ATIC

ATIC 由管理中心服务器和采集器两部分组成，并有两种部署方式。

① 集中式部署：ATIC 服务器和采集器同时安装在同一台物理服务器上。

② 分布式部署：ATIC 服务器和采集器分别安装在不同的物理服务器上，多台采集器可以共用一台 ATIC 服务器，一台 ATIC 服务器最多可管理 20 台采集器。

一台采集器可以处理大约 30 万个 IP 地址的 Anti-DDoS 业务日志，可以根据防护对象的 IP 地址个数来选择 ATIC 部署方式。设备旁路部署时，如果多台设备部署地比较分散，仍然建议配置多台采集器。

本场景的小型数据中心一般采用 ATIC 集中式部署。

10. 路由规划

混插设备、ATIC 管理中心、路由器三者之间要路由可达。

7.2.2 典型组网

如图 7-24 所示，混插设备旁路部署在核心路由器上。分光器与混插设备的检测口相

连，现网流量通过分光器复制到混插设备进行实时检测。混插设备对到达防护对象（内网服务器）的流量进行检测和清洗，当出现攻击时，将到达防护对象的下行流量通过 BGP 引流方式实时牵引至清洗设备进行检测和清洗；清洗完成后，再将正常流量通过策略路由方式回注到原链路 Router 上，最终将流量送到防护对象中。

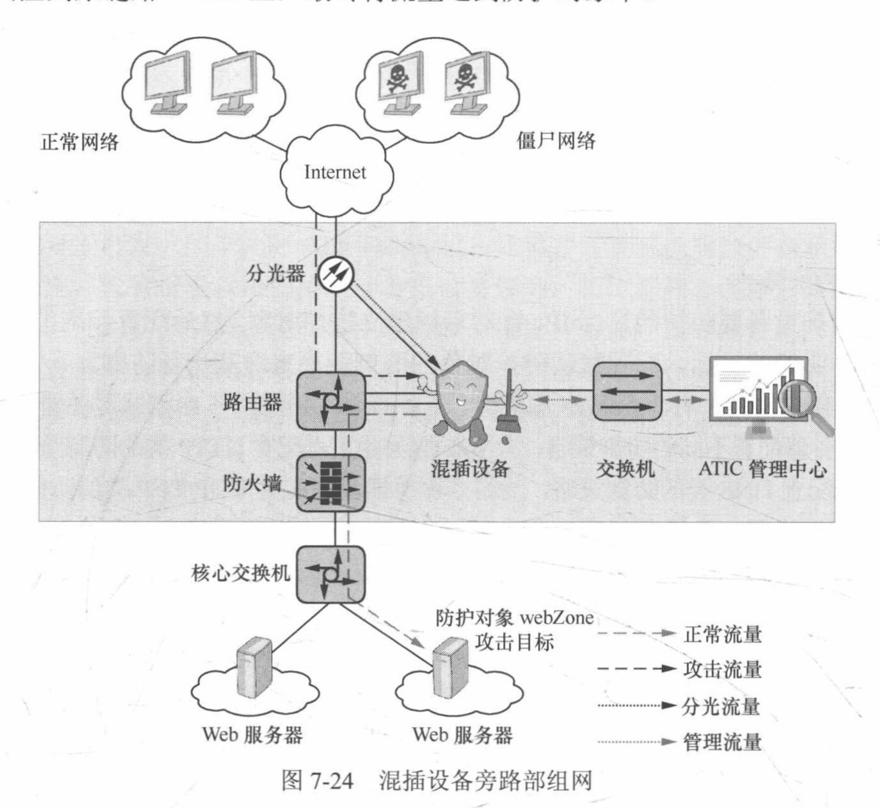


图 7-24 混插设备旁路部组网

7.2.3 数据规划

混插设备、ATIC 和路由器的 IP 地址规划如表 7-4 和图 7-25 所示。

表 7-4 IP 地址规划表

设备名称	接口	IP 地址	说明
混插设备	GE1/0/1	-	检测口
	GE2/0/1	10.1.2.2/24	清洗口 即引流流量入接口，清洗设备对从该口进入的流量应用各种防御策略，对流量进行分析和清洗
	GE2/0/2	10.1.3.2/24	回注口。 清洗后的正常流量通过此接口回注到原链路
	GE3/0/0	10.1.6.1/24	与管理中心的通信口。 清洗设备将日志报文/抓包报文发送至管理中心中的 Anti-DDoS 采集器，供 Anti-DDoS 采集器分析以及进行后续处理。 此接口 IP 地址与管理中心 IP 地址必须路由可达，本例中，此接口 IP 地址与管理中心 IP 地址在同一网段

（续表）

设备名称	接口	IP 地址	说明
ATIC 管理中心	–	10.1.6.2/24	与检测设备、清洗设备路由可达
路由器	GE1/0/1	10.1.2.1/24	引流通道
	GE1/0/2	10.1.3.1/24	回注通道
	GE1/0/3	10.1.5.1/24	与防火墙直连

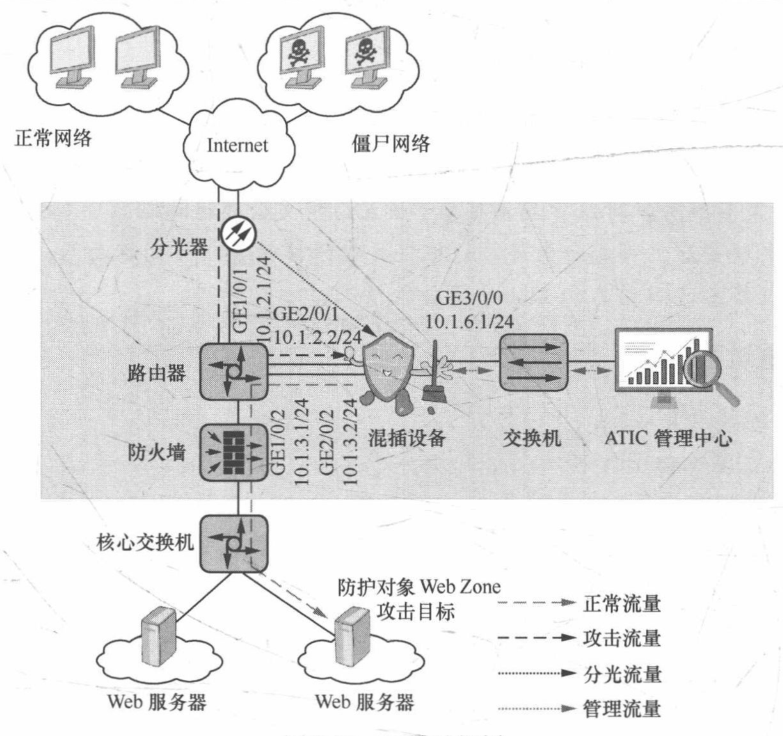


图 7-25 IP 地址规划

路由器的接口 GE1/0/1 与清洗设备的接口 GE2/0/1 之间的通道为引流通道。路由器的接口 GE1/0/2 与清洗设备的接口 GE2/0/2 之间的通道为回注通道。

7.2.4 配置思路

1. 混插设备上的功能配置

① 加载 License。

② 指定业务子卡的类型。

③ 配置接口 IP 地址，接口加入安全区域，并打开域间缺省包过滤。

④ 配置 STelnet 功能。

⑤ 配置 SNMP 功能，使管理中心可以获取清洗设备的状态。

⑥ 配置检测口和清洗口，并在检测口和清洗口开启流量统计功能。

⑦ 配置引流和回注功能。

⑧ 保存配置。

2. ATIC 管理中心的功能配置

① 第一次登录管理中心。

② 创建 Anti-DDoS 设备。

③ 配置相应的防御策略。

④ 配置基线学习功能，并调整防御阈值。

⑤ 保存配置。

另外，现网中还要完成对接路由器的相关配置，本例给出的路由器的配置仅作参考，现网中请根据路由器的具体型号进行配置。

说明 在复杂组网的场景下，请避免以下问题。

■ 在核心路由器使用策略路由指导转发时，当源认证报文被清洗设备回注到路由器后，可能因为查询不到路由而被丢弃，导致源认证失败。

■ 如果多个防护对象有互访关系，且互访报文会经过核心路由器时，在多个互访对象同时发生攻击后，可能会出现源认证报文被清洗设备回注到路由器，之后，又被路由器上的引流路由送回到 Anti-DDoS 设备的情况。

7.2.5 配置过程

1. 配置混插设备

步骤 1 加载 License。

AntiDDoS8000 设备的检测和清洗功能是受 License 控制的，所以用户在购买设备的同时，也要购买相应的 License。License 成功加载并激活是 AntiDDoS8000 设备检测或清洗功能可用的前提条件之一。

License 文件后缀为"*.dat"，License 文件可以被重命名，但扩展名".dat"不能被更改，否则系统将无法正常加载 License 文件。

激活 License 后，可以通过命令 display license，查看 License 的信息。

```
<AntiDDoS> system-view
[AntiDDoS] license active lic_clean_20160530.dat
```

步骤 2 指定业务板子卡使其具备检测和清洗功能。

在缺省情况下，AntiDDoS8000 设备的业务子卡不具备检测或清洗功能，需要通过命令指定。只有与子卡匹配的 License 处于激活状态时，在业务板底板注册成功后，AntiDDoS8000 设备才可以执行下面的命令指定子卡类型。在子卡注册成功后，它才可以继续等待其他配置完成，否则无法进行后续配置。

```
[AntiDDoS] firewall ddos detect-spu slot 4 card 0
[AntiDDoS] firewall ddos clean-spu slot 4 card 1
[AntiDDoS] display ddos slot
Slot ID   Card ID   CPU Number   Config   Register     Status
-------------------------------------------------------------------
4         0         0            detect   Registered   detect
4         1         2            clean    Registered   clean
-------------------------------------------------------------------
```

步骤 3 配置 STelnet 功能。

配置 STelnet 功能是为了实现 ATIC 管理中心对 AntiDDoS8000 设备的管理，比如防御策略的下发、引流策略的下发等。ATIC 和 AntiDDoS8000 的参数配置要保持完全一致。

```
[AntiDDoS] user-interface vty 0 4
[AntiDDoS-ui-vty0-4] authentication-mode aaa
[AntiDDoS-ui-vty0-4] user privilege level 3
[AntiDDoS-ui-vty0-4] protocol inbound ssh
[AntiDDoS-ui-vty0-4] quit
[AntiDDoS] aaa
[AntiDDoS-aaa] manager-user atic
[AntiDDoS-aaa-manager-user-atic] password
Enter Password:
Confirm Password:
[AntiDDoS-aaa-manager-user-atic] service-type ssh
[AntiDDoS-aaa-manager-user-atic] level 15
[AntiDDoS-aaa-manager-user-atic] quit
[AntiDDoS-aaa] quit
[AntiDDoS] rsa local-key-pair create
The key name will be: AntiDDoS_Host
The range of public key size is (512 ~ 2048).
NOTES: A key shorter than 1024 bits may cause security risks.
       The generation of a key longer than 512 bits may take several minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
...++++++++
..++++++++
................................+++++++++
...........+++++++++
[AntiDDoS] stelnet server enable
[AntiDDoS] ssh user atic
[AntiDDoS] ssh user atic authentication-type password
[AntiDDoS] ssh user atic service-type stelnet
```

步骤4 配置接口 IP 地址，并将各接口加入相应的安全区域。

（1）配置接口 IP 地址

在缺省情况下，AntiDDoS8000 接口开启了访问控制管理功能。管理接口（GE0/0/0）下的 HTTP、HTTPS、Ping 权限都是放开的，不需要配置任何安全策略，就能通过管理口访问到设备。非管理口（包括逻辑接口，如 VLANIF、VT 接口、Tunnel 接口）下的 Telnet、Ping、SSH、SNMP 等权限都是关闭的。此时，即使放开了接口所在安全域到 local 的安全策略，非管理接口也不能通过该接口访问设备。非管理接口执行 **undo service-manage enable** 命令后，可以开启接口的 Telnet、Ping、SSH、SNMP 等功能。

```
[AntiDDoS] interface GigabitEthernet 2/0/1
[AntiDDoS-GigabitEthernet2/0/1] undo service-manage enable
[AntiDDoS-GigabitEthernet2/0/1] ip address 10.1.2.2 24
[AntiDDoS-GigabitEthernet2/0/1] quit
[AntiDDoS] interface GigabitEthernet 2/0/2
[AntiDDoS-GigabitEthernet2/0/2] undo service-manage enable
[AntiDDoS-GigabitEthernet2/0/2] ip address 10.1.3.2 24
[AntiDDoS-GigabitEthernet2/0/2] quit
[AntiDDoS] interface GigabitEthernet 3/0/0
[AntiDDoS-GigabitEthernet3/0/0] undo service-manage enable
[AntiDDoS-GigabitEthernet3/0/0] ip address 10.1.6.1 24
[AntiDDoS-GigabitEthernet3/0/0] quit
```

（2）加入安全区域

接口如果不加入安全区域，就会导致业务不通。

```
[AntiDDoS] firewall zone trust
[AntiDDoS-zone-trust] add interface GigabitEthernet 2/0/1
[AntiDDoS-zone-trust] add interface GigabitEthernet 2/0/2
[AntiDDoS-zone-trust] add interface GigabitEthernet 3/0/0
[AntiDDoS-zone-trust] quit
```

步骤 5　打开域间缺省包过滤。

在缺省情况下，AntiDDoS8000 的各域间安全策略是禁止通过的，需要将域间包过滤配置为允许，报文才能正常通过 AntiDDoS8000 设备。在 AntiDDoS8000 设备上，可以不配置严格的安全策略，把所有安全策略打开即可。

```
[AntiDDoS] security-policy
[AntiDDoS-policy-security] default action permit
[AntiDDoS-policy-security] quit
```

步骤 6　配置 SNMP V3 功能。

同时在 AntiDDoS8000 和 ATIC 配置 SNMP 功能，并保证配置参数一致，ATIC 可以获取混插设备的状态信息。

```
[AntiDDoS] acl 2998
[AntiDDoS-acl-basic-2998] rule permit source 10.1.6.2 0 description for snmp access
[AntiDDoS-acl-basic-2998] quit
[AntiDDoS] snmp-agent acl 2998
[AntiDDoS] snmp-agent sys-info version v3
[AntiDDoS] snmp-agent group v3 atic privacy acl 2998
[AntiDDoS] snmp-agent usm-user v3 atic
[AntiDDoS] snmp-agent usm-user v3 atic group atic
[AntiDDoS] snmp-agent usm-user v3 atic authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[AntiDDoS] snmp-agent usm-user v3 atic privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
```

步骤 7　配置检测口。

检测口是 AntiDDoS8000 接收分光或者镜像流量的接口。从这个接口进入 AntiDDoS8000 的流量都是复制流量，该流量只被统计，不被转发。检测口无需配置 IP 地址。

（1）指定接口类型为检测口

AntiDDoS8000 指定检测口后，从检测口进来的报文才会被上送到检测模块进行处理。

```
[AntiDDoS] interface GigabitEthernet 1/0/1
[AntiDDoS-GigabitEthernet1/0/1] anti-ddos detect enable
```

（2）配置接口流量统计功能

流量统计功能是 AntiDDoS8000 对流量进行各种计数统计的前提条件，在检测口务必要开启流量统计功能，否则检测功能不生效。在缺省情况下，接口流量统计功能是关闭状态。

```
[AntiDDoS-GigabitEthernet1/0/1] anti-ddos flow-statistic enable
[AntiDDoS-GigabitEthernet1/0/1] quit
```

步骤 8　配置清洗口。

清洗口一般是指待清洗流量进入 AntiDDoS8000 的接口。在旁路部署的场景中，清洗口是引流流量的入口。从这个接口进入 AntiDDoS8000 的流量，要经过检测模块和清洗模块，所以需要在接口上指定接口类型并配置流量统计功能。

（1）指定接口类型为清洗口

AntiDDoS8000 指定清洗口后，从清洗口进来的报文才会被上送到清洗模块进行处理。

```
[AntiDDoS] interface GigabitEthernet 2/0/1
[AntiDDoS-GigabitEthernet2/0/1] anti-ddos clean enable
```

（2）配置接口流量统计功能

流量统计功能是设备对流量进行各种计数统计的前提条件，在清洗口务必开启流量统计功能，否则清洗功能不生效。在缺省情况下，接口流量统计功能是关闭状态。

```
[AntiDDoS-GigabitEthernet2/0/1] anti-ddos flow-statistic enable
[AntiDDoS-GigabitEthernet2/0/1] quit
```

步骤 9　在 AntiDDoS8000 上，配置动态生成路由时使用的是下一跳地址。

下一跳地址配置是与清洗设备回注接口直连的 Router1 接口 GE1/0/2。当 AntiDDoS8000 的检测模块检测到某个 IP 地址被攻击时，向 ATIC 通告攻击日志。ATIC 收到攻击日志后，会向 AntiDDoS8000 自动下发一条引流命令，这条引流命令和下面配置的下一跳地址命令相结合，就会在 AntiDDoS8000 上生成一条 32 位 UNR 引流路由。这条引流路由会通过 BGP 发布到对端 Router1 上。

这条引流路由要保证在路由器上是优先级最高的路由，否则会导致引流失败。

```
<AntiDDoS> system-view
[AntiDDoS] firewall ddos bgp-next-hop 10.1.3.1
```

步骤 10　在清洗设备上配置 BGP 功能及团体属性。

AntiDDoS8000 和 Router1 之间建立 BGP 关系，Router1 为引流路由器。当 AntiDDoS8000 生成 UNR 引流路由时，会通过 BGP 发布给 Router1，实现引流功能。清洗设备不向其他对等体发布匹配的路由。

```
[AntiDDoS] route-policy 1 permit node 1
[AntiDDoS-route-policy] apply community no-advertise
[AntiDDoS-route-policy] quit
[AntiDDoS] bgp 100
[AntiDDoS-bgp] peer 10.1.2.1 as-number 100
[AntiDDoS-bgp] import-route unr
[AntiDDoS-bgp] ipv4-family unicast
[AntiDDoS-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export
[AntiDDoS-bgp-af-ipv4] peer 10.1.2.1 advertise-community
[AntiDDoS-bgp-af-ipv4] quit
[AntiDDoS-bgp] quit
```

完成上述配置后，清洗设备上生成的 UNR 会被引入到 BGP 中，并通过 BGP 发布到 Router1。当 Router1 收到目的地址为 1.1.1.1/32 的流量时，其通过查路由表，根据最长掩码匹配原则，优先将流量从接口 GE1/0/1 转发至清洗设备。

步骤 11　在清洗设备接口 GE2/0/1 上配置策略路由，实现回注功能。

回注一方面是要把清洗后的流量回注到原链路中，最后再送到防护对象中；另一方面，是要避开引流路由，防止发生路由环路。

```
[AntiDDoS] policy-based-route
[AntiDDoS-policy-pbr] rule name huizhu
```

```
[AntiDDoS-policy-pbr-rule-huizhu] ingress-interface GigabitEthernet 2/0/1
[AntiDDoS-policy-pbr-rule-huizhu] action pbr egress-interface GigabitEthernet 2/0/2 next-hop 10.1.3.1
[AntiDDoS-policy-pbr-rule-huizhu] quit
[AntiDDoS-policy-pbr] quit
```

步骤 12 保存配置。

```
<AntiDDoS> save
```

2. 配置 ATIC

步骤 1 登录 ATIC。

在浏览器中输入管理中心 IP 地址 https://10.1.6.2，按“Enter”键。在登录界面上，输入用户名、密码和验证码。用户名为 admin，密码为 Admin@123。单击“登录”。第一次登录时，要修改初始密码。

步骤 2 创建 Anti-DDoS 设备。

① 选择“防御 > 网络配置 > 设备”。

② 单击 创建 。将混插设备添加到设备列表中，如图 7-26 所示。

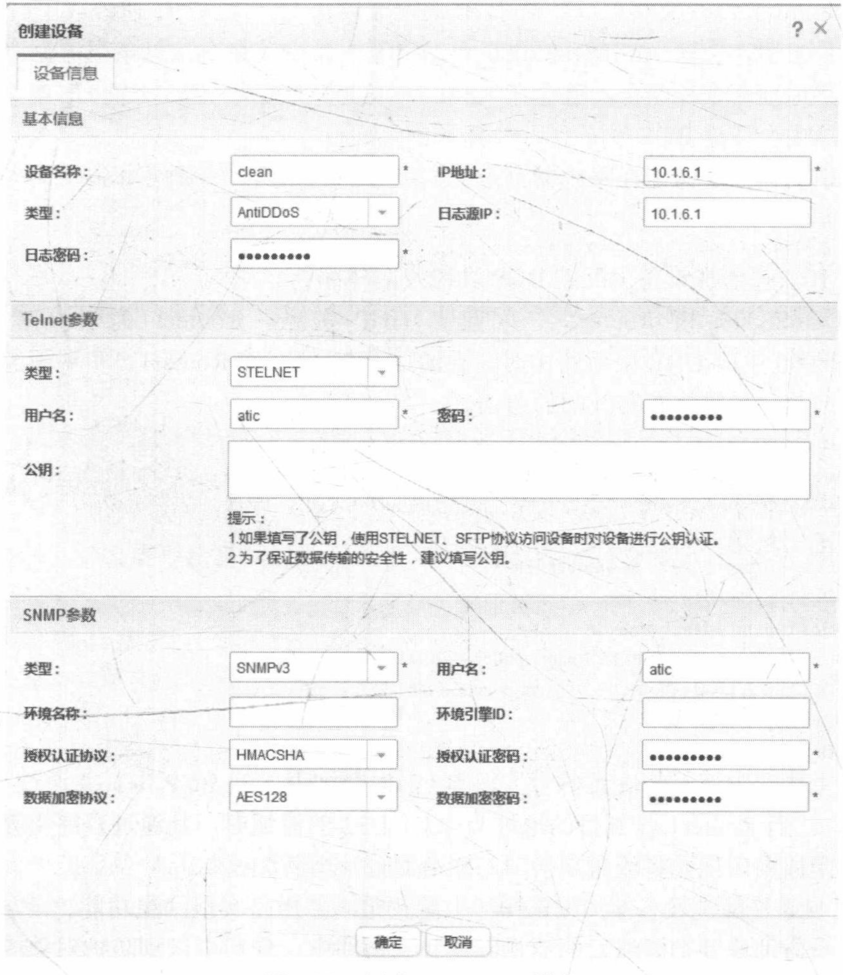


图 7-26 创建 Anti-DDoS 设备

- IP 地址是指 AntiDDoS8000 管理口的 IP 地址。

• 日志源 IP 指 AntiDDoS8000 的日志口 IP 地址。

• 日志密码指上报日志的加密密钥。当设备成功创建后，ATIC 将密钥下发到 Anti-DDoS 设备上。

STelnet 的参数和 SNMP 的参数配置和 AntiDDoS8000 设备的参数配置必须保持完全一致，系统会进行校验。

③ 单击“确定”。

步骤 3　选择“防御 > 策略配置 > 防护对象”，创建自定义防护对象，并配置防护对象的基本信息。

防护对象的 IP 地址是需要保护的服务器 IP 地址。不同业务类型的服务器需创建不同的防护对象。例如：针对 Web 服务器，可创建防护对象 webZone。

步骤 4　配置 Web 服务器的防御策略。

Web 服务器以 HTTP 和 HTTPS 业务为主，UDP 业务流量较少。所以在配置防御策略时，可以考虑配置 TCP、HTTP、HTTPS 的精细防御策略，之后，再直接配置 UDP、ICMP 的限流即可。

① 选择“防御 > 策略配置 > 防护对象”，单击防护对象 webZone 对应的，配置防御模式，如图 7-27 所示。

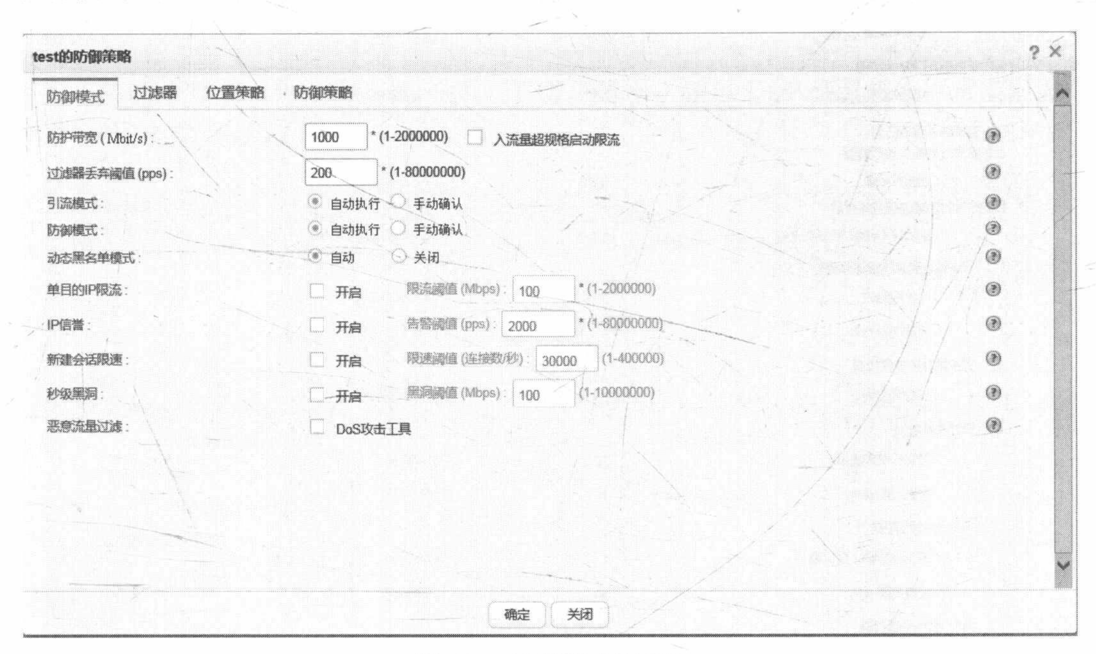


图 7-27　防御模式的配置

② 在“防御策略”页签中，单击以 basic 开头的默认防御策略对应的“操作”列的。

③ TCP 防御：TCP 的基本防御都可以被开启，如图 7-28 所示。

ACK Flood 防御：严格模式的防御效果优于宽松模式。

在直路部署时，推荐使用 ACK Flood 防御的严格模式，业务不会有中断，防御效果也好于宽松模式。

在旁路部署时，建议使用 ACK Flood 防御的宽松模式。因为在旁路部署时使用严格

模式，根据严格模式的防御原理，业务在引流后要求 ACK 报文命中的会话必须是由 SYN 或 SYN-ACK 建立的，否则报文会被丢弃，会话重建后业务才会正常。

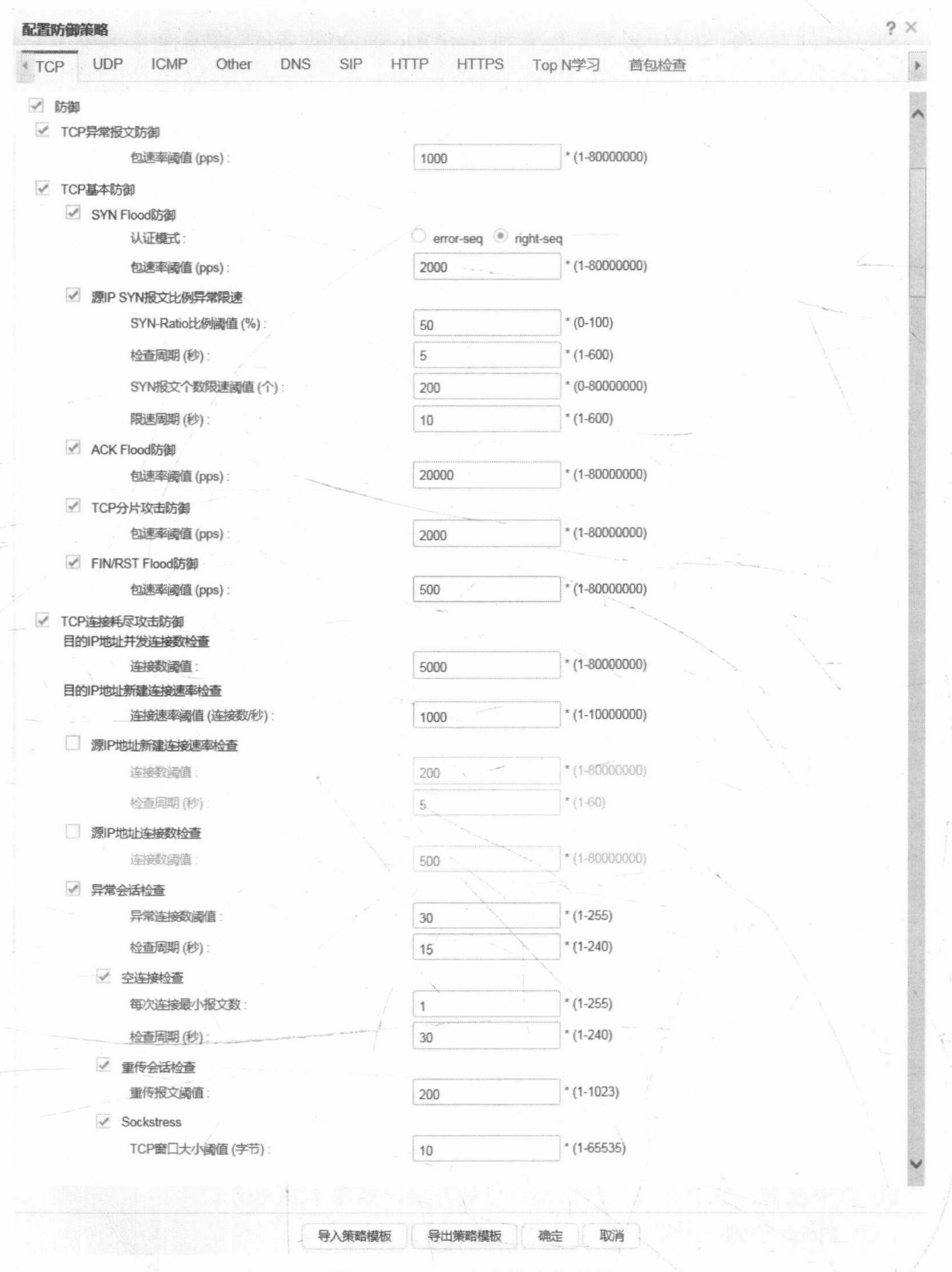


图 7-28 TCP 防御策略的配置

图 7-18 中的配置在攻击时仅能告警，不能清洗，只有配置动态黑名单功能才能进行

清洗，建议在应急的时候再开启动态黑名单功能。开启方法如图 7-29 所示。

LF默认防护对象的防御策略

防御模式　过滤器　位置策略　防御策略

防护带宽 (Mbps)：1000 * (1-2000000)　入流量超规格启动限流

过滤器丢弃阈值 (pps)：100 * (1-80000000)

引流模式：自动执行　手动确认

防御模式：自动执行　手动确认

动态黑名单模式：自动　关闭

单目的IP限流：开启　限流阈值 (Mbps)：100 * (1-2000000)

IP信誉：开启　告警阈值 (pps)：2000 * (1-80000000)

新建会话限速：开启　限速阈值 (连接数/秒)：30000 (1-400000)

秒级黑洞：开启　黑洞阈值 (Mbps)：100 (1-10000000)

恶意流量过滤：DoS攻击工具

确定　关闭

图 7-29　开启动态黑名单

④ UDP 防御：Web 服务器一般没有 UDP 业务，所以 UDP 流量很小，直接限流即可，如图 7-30 所示。



图 7-30　UDP 防御策略的配置

⑤ ICMP 防御：现网中正常情况下只有少量的 Ping 报文，所以 ICMP 的限速阈值可

以配置得小一点，如图 7-31 所示。

图 7-31 ICMP 防御策略的配置

⑥ Other 报文的防御以限流为主，如图 7-32 所示。

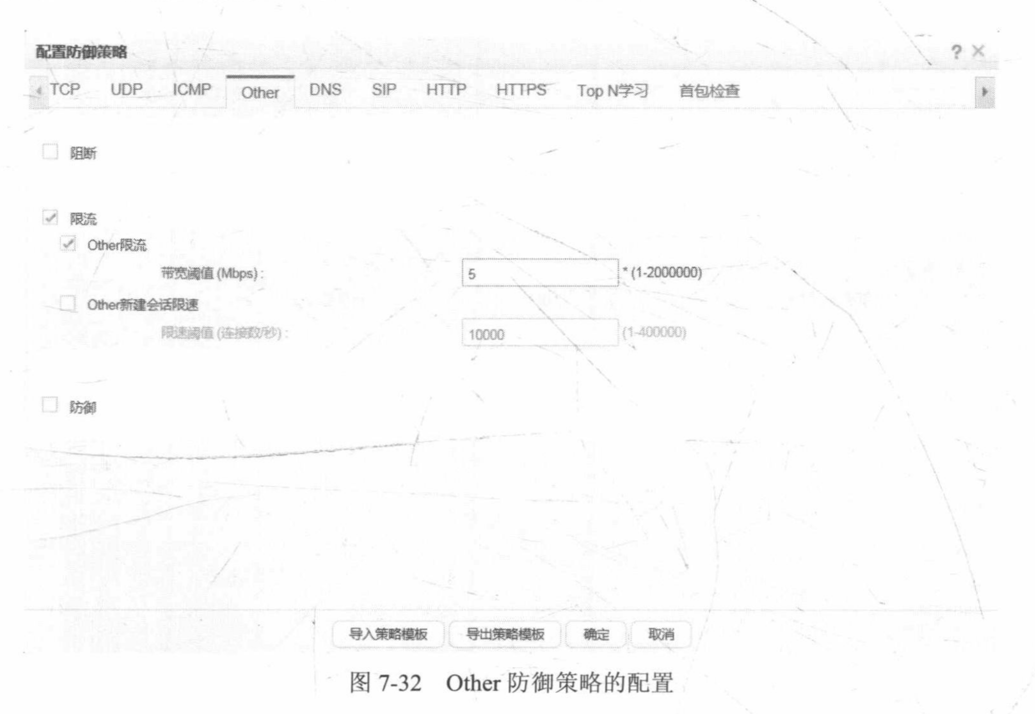


图 7-32 Other 防御策略的配置

⑦ HTTP 源认证防御，如图 7-33 所示。

多数用户的浏览器和 App 都有完整的 HTTP 协议栈，因此可以顺利通过“302 重定向”，

当流量超过阈值触发防御后，用户感知不到认证过程，业务访问没有受到任何影响。但少数个别的 App 和程序可能使用了不完整的 HTTP 协议栈，无法通过 HTTP“302 重定向”的认证，导致业务受到影响，这个时候就需要关闭 HTTP 源认证防御，避免影响正常业务。



图 7-33　HTTP 防御策略的配置

⑧ HTTPS 源认证防御，如图 7-34 所示。



图 7-34　HTTPS 防御策略的配置

⑨ 过滤器配置：除上述防御策略以外，对于不提供服务的端口，可以通过配置过滤器进行阻断。

单击“过滤器”，进入页签后，单击 关联过滤器 。选中 ATIC 缺省提供的除“DNS_Amplification”外的所有过滤器模板，单击“确定”。

步骤 5 部署防御策略。

① 选择“防御 > 策略配置 > 防护对象”，选中防护对象前的复选框，单击 部署。

② 单击“确定”，显示部署的进度提示，部署完成后进度提示自动关闭。

步骤 6 选择“防御 > 策略配置 > 防护对象”，单击“基线学习状态”列的具体状态，开启基线学习功能，如图 7-35 所示。

基线学习不需要配置策略，只要有流量经过设备即可。

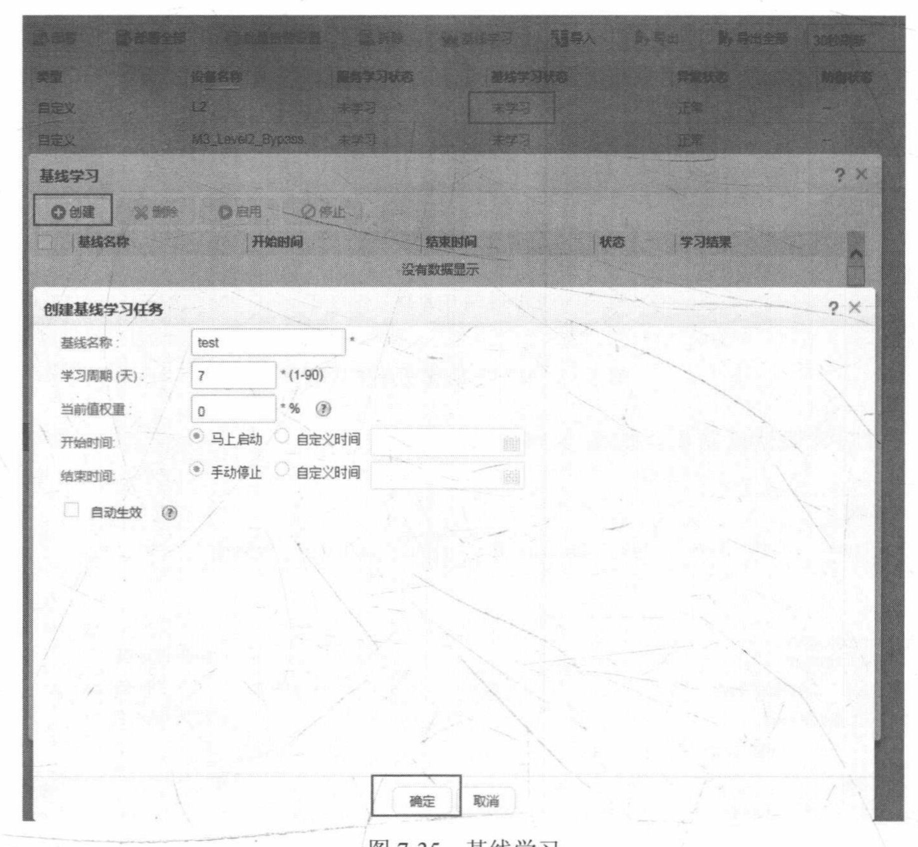


图 7-35 基线学习

步骤 7 调整阈值。

一般情况下，如果应用基线学习到数据之后，告警会比较多，因此，需要适当调整阈值或者其他参数。

① 将抽样比调整为 0，即每个报文都统计。如果抽样比配置过大，当流量比较小时，统计出来的值容易失真和跳变。一般情况下，如果总流量小于 1GB，都可以将抽样比配置为 0。

② 查看该防护对象的流量 TopN（无攻击的情况下），选取流量最大的 IP，并以此

IP 查看各种协议的流量对比（统计方式选择峰值），时间跨度选择一周即可。然后使用每种流量峰值的 2 倍作为相应防范的阈值。如果流量峰值比较小，比如只有几十 pps，建议直接使用默认值作为阈值，真正发生攻击之后，攻击流量不可能才只有几千 pps。

步骤 8 保存配置。

① 选择“防御 > 策略配置 > 设备全局配置”，选中 Anti-DDoS 设备前的复选框，单击 保存设备配置 。

② 单击“确定”，显示保存的进度提示，完成保存后进度提示自动关闭。

3. 路由器配置过程

下面以华为路由器 NE80E 为例，介绍路由器的 BGP 和策略路由的配置过程。不同版本的路由器的配置不同，请根据实际路由器版本进行配置，以下配置仅供参考。

步骤 1 配置路由器接口的 IP 地址。

步骤 2 配置路由器的 BGP 功能。

```
[Router1] bgp 100
[Router1-bgp] peer 10.1.2.2 as-number 100
[Router1-bgp] quit
```

步骤 3 在路由器接口 GE1/0/2 配置策略路由。

① 定义流分类。

```
[Router1] acl 3001
[Router1-acl-adv-3001] rule permit ip
[Router1-acl-adv-3001] quit
[Router1] traffic classifier class1
[Router1-classifier-class1] if-match acl 3001
[Router1-classifier-class1] quit
```

② 配置流行为并配置报文转发动作。

```
[Router1] traffic behavior behavior1
[Router1-behavior-behavior1] redirect ip-nexthop 10.1.5.2 interface GigabitEthernet 1/0/3
[Router1-behavior-behavior1] quit
```

③ 定义流量策略并在策略中为类指定行为。

```
[Router1] traffic policy policy1
[Router1-trafficpolicy-policy1] classifier class1 behavior behavior1
[Router1-trafficpolicy-policy1] quit
```

④ 在接口上应用策略路由。

```
[Router1] interface GigabitEthernet 1/0/2
[Router1-GigabitEthernet1/0/2] traffic-policy policy1 inbound
[Router1-GigabitEthernet1/0/2] quit
```

7.3 大型数据中心防护

相比于小型数据中心，大型数据中心（IDC）不仅仅是一个网络的概念，更是一个服务的概念，它已成为网络基础资源的一部分，如图 7-36 所示。IDC 通常为 ICP（互联网内容提供商）、企业、媒体和各大网站提供大规模、高质量的专业服务器托管、空间租用网络带宽批发等传输和接入服务。企业将 IT 设施外包给专业的 IDC

服务提供商，IDC 服务提供商向企业提供设备的维护和管理、机房设施、带宽服务以及应用服务。这种专业化的服务减少了资源的投入，从而降低了传统企业上网的门槛。

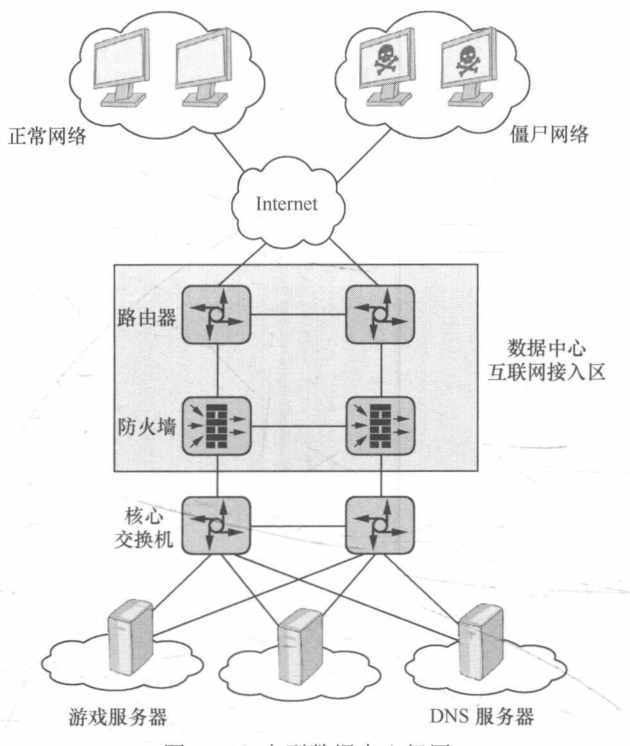


图 7-36 大型数据中心组网

随着 IDC 的广泛应用，IDC 的网络安全也变得更加重要。针对 IDC 的流量特点，我们规划网络时应从以下几个方面考虑。

7.3.1 规划思路

1．设备选择

数据中心有储存各种重要业务信息的服务器，这些服务器承载了现网中的各种业务，服务器一旦受到攻击，会直接导致部分网络瘫痪，直接影响正常业务，所以数据中心的检测和清洗精准度非常重要。华为 AntiDDoS8000 设备采用的是逐包检测技术。相比于逐流检测，逐包检测更精细，同时也可针对不同的业务配置差异化防御策略。逐包检测的防御更精准，推荐使用。

2．部署方式

旁路部署方式不改变原有网络的拓扑结构，保证了链路的可靠性。

大型数据中心业务量大，对设备性能要求高，建议分别独立部署 1 台 AntiDDoS8000 检测设备和 1 台清洗设备。

3．流量引导方式

数据中心组网不会很复杂，回注链路也不会太多，建议采用 BGP 旁路引流+策略路

由回注方式引导流量流回 Anti-DDoS 设备。BGP 引流可以实现动态引流，策略路由回注的配置简单。

Anti-DDoS 设备既支持静态引流，又支持动态引流。静态引流清洗是指不管是否发生攻击，Anti-DDoS 设备都将所有流量引导到清洗设备中，再由清洗设备转发。当发生攻击时，清洗过程会非常消耗清洗设备的性能。一旦清洗设备性能达到瓶颈，就会影响流量的转发。如果此时 Anti-DDoS 设备还有其他用户的流量需要转发，只要设备性能稍有问题，没有遭受攻击的用户业务也会受到影响。相比于静态引流方式，动态引流可靠性更高。使用动态引流，没有发生攻击时，流量并不会经过清洗设备。只有当攻击发生后，清洗设备才会将去往被攻击用户的流量引流到设备上进行清洗，其他未受到攻击的用户的流量不会被引流，也不会经过清洗设备。因此，即使清洗设备流量很大也不会影响其他用户。

4. 业务子卡规划

AntiDDoS8000 是分布式设备，设备是检测设备还是清洗设备取决于业务子卡的类型。在缺省情况下，AntiDDoS8000 业务板的子卡不具有检测或清洗功能，用户需要通过命令指定某槽位业务子卡的功能是检测功能还是清洗功能。

5. License 控制

AntiDDoS8000 业务板的子卡同时也受 License 控制，命令制定后，其要加载相匹配的 License，才能生效。AntiDDoS8000 的检测和清洗 License 控制项见表 7-5。

表 7-5　AntiDDoS8000 的检测和清洗 License 控制项

资源项	适配的子卡	功能
检测子卡-20	只能加载在 ADS-SPC-20-00 业务子卡上	激活 License 后，检测功能可用
检测子卡-40	只能加载在 ADS-SPC-40-00 业务子卡上	激活 License 后，检测功能可用
检测子卡-80	只能加载在 ADS-SPC-80-00 业务子卡上	激活 License 后，检测功能可用
清洗子卡-20	只能加载在 ADS-SPC-20-00 业务子卡上	激活 License 后，清洗功能可用
清洗子卡-40	只能加载在 ADS-SPC-40-00 业务子卡上	激活 License 后，清洗功能可用
清洗子卡-80	只能加载在 ADS-SPC-80-00 业务子卡上	激活 License 后，清洗功能可用

AntiDDoS8000 支持使用主控板 ESN 和背板 ESN 申请 License。主控板的 ESN 可以使用命令 display esn 查询，背板的 ESN 可以使用 display esn all 查询，显示的 BackPlane 为背板的 ESN，也可以使用 display license esn 查询。我们推荐使用背板 ESN 申请 License。因为主控板故障率比背板的高，更换以后需要重新申请 License，以及双主控情况下需要使用两个 ESN，任何一个主控板故障都要更换 license。

在双主控的情况下，AntiDDoS8000 必须同时提供主备主控板的 ESN。假如只使用主用主控板的 ESN 申请并激活 License 文件，则需要重新使用主用主控板和备用主控板的 ESN 去申请 License 文件，取消已经激活的 License 文件，再激活新的 License 文件即可正常使用。

6. 检测设备接口规划

规划检测设备时需要规划一个检测口、一个管理口、一个与 ATIC 通信的管理口和一个日志口。

检测口用于接收分光或者镜像的流量，从这个接口进入检测设备的流量都是网络中的复制流量。

独立检测设备的管理口和清洗设备、混插设备的管理口不同，需要单独配置一条管理口命令：anti-ddos detect-device manage-port enable。当独立部署检测设备时，在缺省情况下，检测设备接收到的报文都被认为是分光或者镜像的报文，只做流量统计，统计完成后直接被丢弃，不被转发。对于检测设备的管理流量，比如，检测设备通过 SSH 或 Telnet 等方式管理设备的流量时，如果不特殊配置的话，也会被丢弃。所以需要在检测设备上配置管理口用于管理设备，这样，从管理口接收的流量就不会被丢弃，而会被继续上送处理。

管理口和日志口可以是同一个接口，也可以是不同的接口。主控板接口 GigabitEthernet0/0/0 可以作为与 ATIC 通信的管理接口，但不能作为向 ATIC 发送日志的接口。所以如果管理口和日志口用同一个接口的话，就不能用 GigabitEthernet0/0/0 接口。

ATIC 服务器只有 GE 接口，建议在接口板预留 1 个 GE 接口与 ATIC 互连。如果 AntiDDoS8000 设备上只有 10GE 接口，也可以使用中间网络设备进行 GE 接口与 10GE 接口的转换。

7. 清洗设备接口规划

清洗设备需要规划一个清洗口（引流口）、一个回注口、一个与 ATIC 通信的管理口和一个日志口。其中，引流口和回注口可以是两个不同的主接口，也可以是一个主接口下的两个子接口。

8. 防御策略

首先明确设备要防护的目标 IP，针对目标建立防护对象，然后配置相应的防护策略。对于其他不明确的目标，需要配置默认防护对象的防御策略来防御。

例如：IDC 网络中有 3 台 Web 服务器、2 台 DNS 服务器以及 5 台游戏服务器。不同的服务器配置不同的防御策略，像 Web 服务器重点配置 HTTP 类的防御策略，DNS 服务器则重点配置 DNS 类的防御策略，游戏服务器则重点配置 UDP/TCP 类的防御策略。

如果我们为每一个服务器建立一个防护对象，则需要建立 10 个防护对象，配置起来比较麻烦。如果同一类型的服务器业务基本相同，则可以只配置 3 个防护对象，即针对 Web 服务器、DNS 服务器和游戏服务器的 3 个防护对象；然后，在每一个防护对象中将多个服务器的 IP 地址添加进来（每个防护对象可以配置多个 IP 或者网段）；最后再配置相应的防御策略，这样每一类服务器只需要配置一次策略。

配置完成后，就完成了重点目标的防护，我们也可以对 IDC 中其他的网络资源使用默认防护对象的防御策略来进行防御。

9. 安全策略规划

在缺省情况下，AntiDDoS8000 设备上的安全策略是关闭的，但可以打开缺省包过滤。

10. ATIC

ATIC 由管理中心服务器和采集器两部分组成，并有两种部署方式。

① 集中式部署：ATIC 服务器和采集器同时安装在同一台物理服务器上。

② 分布式部署：ATIC 服务器和采集器分别安装在不同的物理服务器上，多台采集器可以共用一台 ATIC 服务器，一台 ATIC 服务器最多可管理 20 台采集器。

一台采集器大约可以处理 30 万个 IP 地址的 Anti-DDoS 业务日志，可以根据防护对象的 IP 地址个数来选择 ATIC 部署方式。设备旁路部署时，如果多台设备部署地比较分散，则建议配置多台采集器。

在本例中，管理中心采用集中式部署，即采集器与管理服务器部署在同一台服务器上。

11. 路由规划

检测设备、清洗设备、ATIC 三者之间要路由可达。

7.3.2 典型组网

如图 7-37 所示，清洗设备旁路部署在 Router1 和 Router2 上，检测和清洗到达防护对象的流量。由于是旁路部署，因此需要将到达防护对象的下行流量通过 BGP 引流方式实时牵引至清洗设备进行检测和清洗，清洗完成后，再将正常流量通过策略路由方式回注到原链路 Router1 和 Router2 上，最终将流量送到防护对象中。

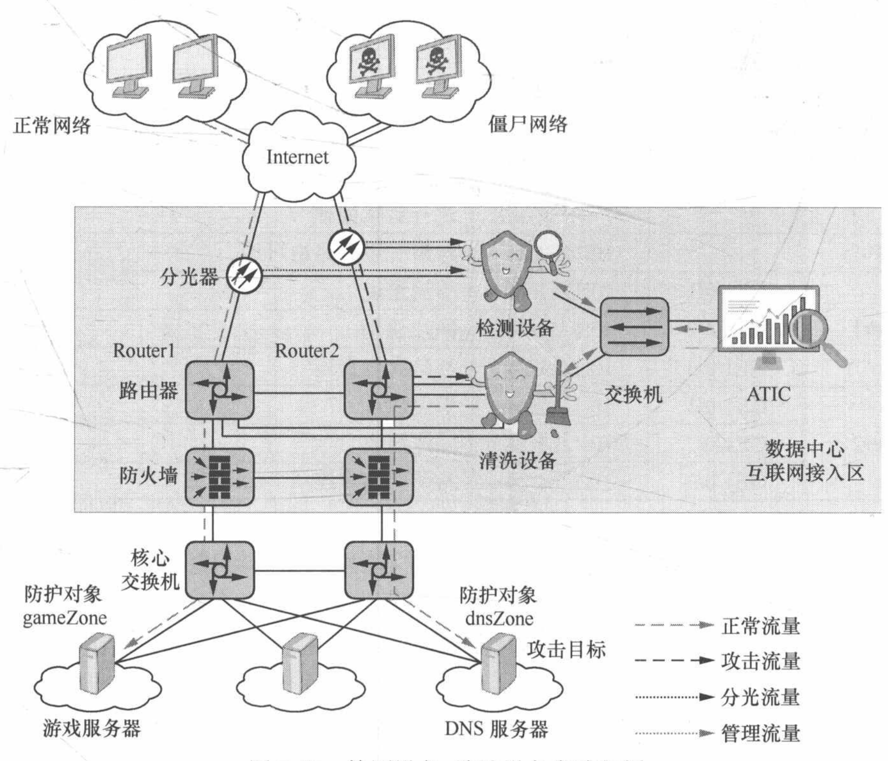


图 7-37 检测设备+清洗设备旁路部署

7.3.3 数据规划

清洗设备和管理中心的 IP 地址规划如表 7-6 和图 7-38 所示。

表 7-6 IP 地址规划

设备名称	接口	IP 地址	说明
检测设备	GE2/0/1	-	检测口
	GE2/0/2	-	检测口
	GE3/0/0	10.1.6.3/24	与管理中心通信口 检测设备一起将日志报文/抓包报文发送至管理中心中的 Anti-DDoS 采集器，供 Anti-DDoS 采集器分析以及进行后续处理。 此接口 IP 地址与管理中心 IP 地址必须路由可达，在本例中，此接口 IP 地址与管理中心 IP 地址在同一网段
清洗设备	GE1/0/1	10.1.0.2/24	与 Router1 直连清洗口（引流流量入接口），清洗设备对从该口进入的流量应用各种防御策略，对流量进行分析和清洗
	GE1/0/2	10.1.1.2/24	与 Router1 直连回注口。 清洗后的正常流量通过此接口回注到原链路
	GE2/0/1	10.1.2.2/24	与 Router2 直连清洗口（引流流量入接口），清洗设备对从该口进入的流量应用各种防御策略，对流量进行分析和清洗
	GE2/0/2	10.1.3.2/24	与 Router2 直连回注口。 清洗后的正常流量通过此接口回注到原链路
	GE3/0/0	10.1.6.1/24	与管理中心通信口 清洗设备将日志报文/抓包报文发送至管理中心的 Anti-DDoS 采集器，供 Anti-DDoS 采集器分析以及进行后续处理
管理中心	–	10.1.6.2/24	与清洗设备路由可达
Router1	GE1/0/1	10.1.0.1/24	引流通道
	GE1/0/2	10.1.1.1/24	回注通道
	GE1/0/3	10.1.4.1/24	与防火墙直连
Router2	GE1/0/1	10.1.2.1/24	引流通道
	GE1/0/2	10.1.3.1/24	回注通道
	GE1/0/3	10.1.5.1/24	与防火墙直连

Router1 的接口 GE1/0/1 与清洗设备的接口 GE1/0/1 之间的通道为引流通道。

Router1 的接口 GE1/0/2 与清洗设备的接口 GE1/0/2 之间的通道为回注通道。

Router2 的接口 GE1/0/1 与清洗设备的接口 GE2/0/1 之间的通道为引流通道。

Router2 的接口 GE1/0/2 与清洗设备的接口 GE2/0/2 之间的通道为回注通道。

管理中心采用集中式部署，即 Anti-DDoS 采集器与管理服务器部署在同一台服务器上。

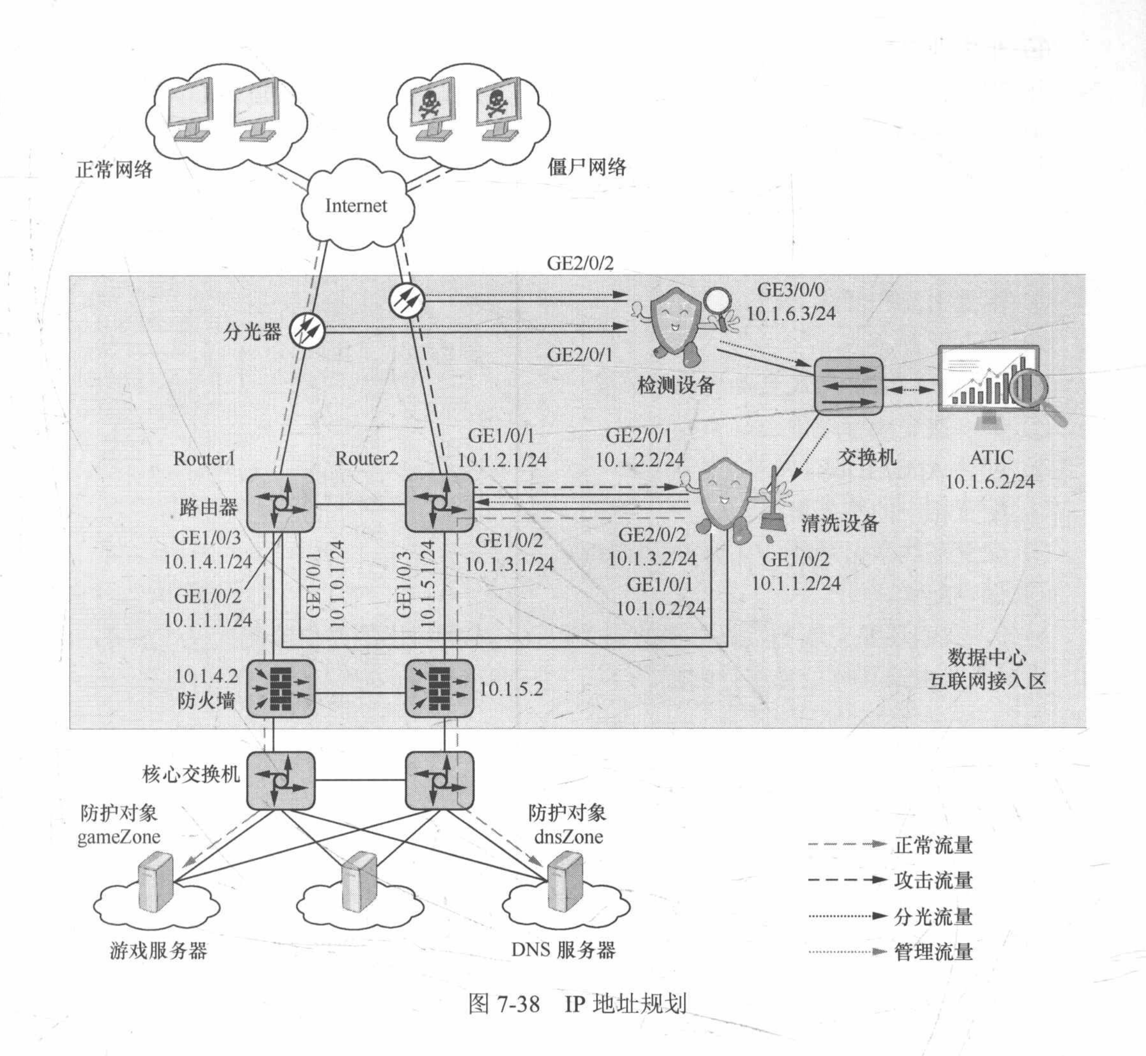


图 7-38　IP 地址规划

7.3.4　配置思路

1．检测设备上需要完成以下主要功能的配置

① 加载 License。

② 指定业务子卡的类型。

③ 配置接口 IP 地址，接口加入安全区域，并打开域间缺省包过滤。其中，检测口无需配置 IP 地址。

④ 配置管理口功能。

⑤ 配置 STelnet 功能。

⑥ 配置 SNMP 功能，使管理中心可以获取检测设备的状态。

⑦ 配置检测口，并在检测口开启流量统计功能。

⑧ 保存配置。

2．清洗设备上需要完成主要功能的配置

① 加载 License。

② 指定业务子卡的类型。

③ 配置接口 IP 地址，接口被加入安全区域，并打开域间缺省包过滤。

④ 配置 STelnet 功能。

⑤ 配置 SNMP 功能，使管理中心可以获取清洗设备的状态。

⑥ 配置清洗口，并在清洗口开启流量统计功能。

⑦ 引流口和回注口配置 Link-Group 功能，增强链路可靠性。

⑧ 配置引流和回注功能。

⑨ 保存配置。

3. 管理中心需要完成主要功能的配置

① 第一次登录管理中心。

② 创建 Anti-DDoS。

③ 配置相应的防御策略。

④ 配置基线学习功能，并调整防御阈值。

⑤ 保存配置。

另外，我们还要完成对接路由器的相关配置，本例给出的路由器配置仅作参考，现网中请根据路由器具体型号进行配置。

7.3.5 配置过程

1. 配置检测设备

步骤 1 加载 License。

AntiDDoS8000 的检测功能是受 License 控制的，所以用户在购买设备的同时，也要购买相应的 License。License 成功加载并激活是 AntiDDoS8000 检测功能可用的前提条件之一。

License 文件后缀为“*.dat”，License 文件可以被重命名，但扩展名“.dat”不能被更改，否则系统将无法正常加载 License 文件。

用户激活 License 后，可以通过命令“display license”，查看 License 的信息。

```
<Detect> system-view
[Detect] license active lic_detect_20160530.dat
```

步骤 2 指定业务板子卡的检测功能。

在缺省情况下，AntiDDoS8000 的业务子卡不具备检测功能，需要通过命令指定。只有与子卡匹配的 License 处于激活状态且业务板底板注册成功后，它才可以执行下面的命令指定子卡类型。上述操作非常重要，子卡注册成功后，才可以继续进行接口等其他配置，否则无法进行后续配置。

```
[Detect] firewall ddos detect-spu slot 4 card 0
[Detect] firewall ddos detect-spu slot 4 card 1
[Detect] display ddos slot
Slot ID   Card ID   CPU Number   Config   Register      Status
---------------------------------------------------------------------------------
4         0         0            detect   Registered    detect
4         1         2            detect   Registered    detect
---------------------------------------------------------------------------------
```

步骤3　配置 STelnet 功能。

配置 STelnet 功能是为了实现 ATIC 管理检测设备，比如防御策略的下发、引流策略的下发等。ATIC 和检测设备的 STelnet 参数配置要保持完全一致。

```
[Detect] user-interface vty 0 4
[Detect-ui-vty0-4] authentication-mode aaa
[Detect-ui-vty0-4] user privilege level 3
[Detect-ui-vty0-4] protocol inbound ssh
[Detect-ui-vty0-4] quit
[Detect] aaa
[Detect-aaa] manager-user atic
[Detect-aaa-manager-user-atic] password
Enter Password:
Confirm Password:
[Detect-aaa-manager-user-atic] service-type ssh
[Detect-aaa-manager-user-atic] level 15
[Detect-aaa-manager-user-atic] quit
[Detect-aaa] quit
[Detect] rsa local-key-pair create
The key name will be: AntiDDoS_Host
The range of public key size is (512 ~ 2048).
NOTES: A key shorter than 1024 bits may cause security risks.
        The generation of a key longer than 512 bits may take several minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
...++++++++
..++++++++
.................................+++++++++
...........+++++++++
[Detect] stelnet server enable
[Detect] ssh user atic
[Detect] ssh user atic authentication-type password
[Detect] ssh user atic service-type stelnet
```

步骤4　配置管理口 IP 地址，并将各接口加入相应的安全区域。

在缺省情况下，AntiDDoS8000 接口开启了访问控制管理功能。管理接口（GE0/0/0）下 HTTP、HTTPS、Ping 的权限都是放开的，不需要配置任何安全策略，就能通过管理口访问到设备。非管理口（包括逻辑接口，如 VLANIF、VT 接口、Tunnel 接口）下 Telnet、Ping、SSH、SNMP 等的权限都是关闭的。此时，即使放开了接口所在安全域到 local 的安全策略，也不能通过该接口访问设备。在执行 **undo service-manage enable** 命令后，可以开启接口的 Telnet、Ping、SSH、SNMP 等功能。

```
[Detect] interface GigabitEthernet 3/0/0
[Detect-GigabitEthernet3/0/0] undo service-manage enable
[Detect-GigabitEthernet3/0/0] ip address 10.1.6.3 24
# 指定接口类型，从此接口进入的流量才能正常上送到检测模块。
[Detect-GigabitEthernet3/0/0] anti-ddos detect enable
# 配置管理口。
```

当独立部署检测设备时，在缺省情况下，检测设备接收的报文都被认为是分光或者镜像的报文，只做流量统计，统计完成后直接被丢弃，不转发。对于检测设备管理的流量，比如通过 SSH 或 Telnet 等方式对设备进行管理的流量，如果不被特殊配置，也会被

丢弃。所以需要在检测设备上配置管理口用于管理设备，这样，从管理口接收的流量就不会被丢弃，而会被继续上送处理。

```
[Detect-GigabitEthernet3/0/0] anti-ddos detect-device manage-port enable
[Detect-GigabitEthernet3/0/0] quit
```

加入安全区域。如果接口不加入安全区域，会导致业务不通。

```
[Detect] firewall zone trust
[Detect-zone-trust] add interface GigabitEthernet 2/0/1
[Detect-zone-trust] add interface GigabitEthernet 2/0/2
[Detect-zone-trust] add interface GigabitEthernet 3/0/0
[Detect-zone-trust] quit
```

步骤 5　打开域间缺省包过滤。

在缺省情况下，检测设备的各域间安全策略是禁止通过的，需要配置域间包过滤为允许，报文才能正常通过检测设备。在检测设备上，可以不配置严格安全策略，把所有安全策略打开即可。

```
[Detect] security-policy
[Detect-policy-security] default action permit
[Detect-policy-security] quit
```

步骤 6　配置 SNMP V3 功能。

要同时在检测设备和 ATIC 配置 SNMP 功能，并保证配置参数一致，这样 ATIC 才可以获取检测设备的状态信息。

```
[Detect] acl 2998
[Detect-acl-basic-2998] rule permit source 10.1.6.2 0 description for snmp access
[Detect-acl-basic-2998] quit
[Detect] snmp-agent acl 2998
[Detect] snmp-agent sys-info version v3
[Detect] snmp-agent group v3 atic privacy acl 2998
[Detect] snmp-agent usm-user v3 atic
[Detect] snmp-agent usm-user v3 atic group atic
[Detect] snmp-agent usm-user v3 atic authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[Detect] snmp-agent usm-user v3 atic privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
```

步骤 7　配置检测口。

检测口是 AntiDDoS8000 接收分光或者镜像流量的接口。从这个接口进入 AntiDDoS8000 的流量都是复制流量，只进行统计，不转发。检测口无需配置 IP 地址。

流量统计功能是 AntiDDoS8000 对流量进行各种计数统计的前提条件，在检测口务必开启流量统计功能，否则检测功能不生效。在缺省情况下，接口流量统计功能为关闭状态。

```
[Detect] interface GigabitEthernet 2/0/1
[Detect-GigabitEthernet2/0/1] anti-ddos detect enable
[Detect-GigabitEthernet2/0/1] anti-ddos flow-statistic enable
[Detect-GigabitEthernet2/0/1] quit
[Detect] interface GigabitEthernet 2/0/2
```

```
[Detect-GigabitEthernet2/0/2] anti-ddos detect enable
[Detect-GigabitEthernet2/0/2] anti-ddos flow-statistic enable
[Detect-GigabitEthernet2/0/2] quit
```

步骤8　保存配置，配置时要随时保存，以免丢失。

```
<Detect> save
```

2. 配置清洗设备

步骤1　加载License。

AntiDDoS8000的清洗功能是受License控制的，所以用户在购买设备的同时，也要购买相应的License。License成功加载并激活，是AntiDDoS8000清洗功能可用的前提条件之一。

License文件后缀为“*.dat”，License文件可以被重命名，但扩展名为“.dat”不能被更改，否则系统将无法正常加载License文件。

激活License后，可以通过命令display license，查看License的信息。

```
<Clean> system-view
[Clean] license active lic_clean_20160530.dat
```

步骤2　指定业务板子卡为清洗。

在缺省情况下，AntiDDoS8000的业务子卡不具备清洗功能，需要通过命令指定清洗。只有与子卡匹配的License处于激活状态，业务板底板注册成功后，才可以执行下面的命令指定子卡类型。子卡注册成功后，才可以继续进行接口等其他配置，否则无法进行后续配置。

```
[Clean] firewall ddos clean-spu slot 4 card 0
[Clean] firewall ddos clean-spu slot 4 card 1
[Clean] display ddos slot
Slot ID  Card ID  CPU Number  Config  Register    Status
-----------------------------------------------------------------------------------
4        0        0           clean   Registered  clean
4        1        2           clean   Registered  clean
-----------------------------------------------------------------------------------
```

步骤3　配置STelnet功能。

配置STelnet功能是为了实现ATIC对清洗设备的管理，比如防御策略的下发、引流策略的下发等。ATIC和清洗设备的STelnet参数配置要保持完全一致。

```
[Clean] user-interface vty 0 4
[Clean-ui-vty0-4] authentication-mode aaa
[Clean-ui-vty0-4] user privilege level 3
[Clean-ui-vty0-4] protocol inbound ssh
[Clean-ui-vty0-4] quit
[Clean] aaa
[Clean-aaa] manager-user atic
[Clean-aaa-manager-user-atic] password
Enter Password:
Confirm Password:
[Clean-aaa-manager-user-atic] service-type ssh
[Clean-aaa-manager-user-atic] level 15
[Clean-aaa-manager-user-atic] quit
[Clean-aaa] quit
[Clean] rsa local-key-pair create
The key name will be: AntiDDoS_Host
```

```
The range of public key size is (512 ~ 2048).
NOTES: A key shorter than 1024 bits may cause security risks.
        The generation of a key longer than 512 bits may take several minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
...++++++++
..++++++++
.................................+++++++++
...........+++++++++
[Clean] stelnet server enable
[Clean] ssh user atic
[Clean] ssh user atic authentication-type password
[Clean] ssh user atic service-type stelnet
```

步骤 4　配置接口 IP 地址，并将各接口加入相应的安全区域。

配置接口 IP 地址，并将引流口和回注口绑定 Link-group，增强链路可靠性。

在缺省情况下，AntiDDoS8000 接口开启了访问控制管理功能。管理接口（GE0/0/0）下 HTTP、HTTPS、Ping 的权限都是放开的，不需要配置任何安全策略，就能通过管理口访问到设备。非管理口（包括逻辑接口，如 VLANIF、VT 接口、Tunnel 接口）下 Telnet、Ping、SSH、SNMP 等的权限都是关闭的。此时，即使放开了接口所在安全域到 local 的安全策略，也不能通过该接口访问设备。执行 **undo service-manage enable** 命令后，可以开启接口的 Telnet、Ping、SSH、SNMP 等功能。

Link-group 功能是将多个接口的状态相互绑定，组成一个逻辑组。当组内任一接口出现故障时，系统将组内其他接口状态设置为 Down。当组内所有接口恢复正常后，整个组内的接口状态再重新被设置为 Up。绑定 link-group，可以使 2 个清洗口和 2 个回注口的接口状态保持一致。当其中一个接口状态为 Down 时，所有接口的状态都设置为 Down，取消引流，保障链路可靠性。

```
[Clean] interface GigabitEthernet 1/0/1
[Clean-GigabitEthernet1/0/1] undo service-manage enable
[Clean-GigabitEthernet1/0/1] ip address 10.1.0.2 24
[Clean-GigabitEthernet1/0/1] link-group 1
[Clean-GigabitEthernet1/0/1] quit
[Clean] interface GigabitEthernet 1/0/2
[Clean-GigabitEthernet1/0/2] undo service-manage enable
[Clean-GigabitEthernet1/0/2] ip address 10.1.1.2 24
[Clean-GigabitEthernet1/0/2] link-group 1
[Clean-GigabitEthernet1/0/2] quit
[Clean] interface GigabitEthernet 2/0/1
[Clean-GigabitEthernet2/0/1] undo service-manage enable
[Clean-GigabitEthernet2/0/1] ip address 10.1.2.2 24
[Clean-GigabitEthernet2/0/1] link-group 2
[Clean-GigabitEthernet2/0/1] quit
[Clean] interface GigabitEthernet 2/0/2
[Clean-GigabitEthernet2/0/2] undo service-manage enable
[Clean-GigabitEthernet2/0/2] ip address 10.1.3.2 24
[Clean-GigabitEthernet2/0/2] link-group 2
[Clean-GigabitEthernet2/0/2] quit
[Clean] interface GigabitEthernet 3/0/0
[Clean-GigabitEthernet3/0/0] undo service-manage enable
```

```
[Clean-GigabitEthernet3/0/0] ip address 10.1.6.1 24
[Clean-GigabitEthernet3/0/0] quit
```

加入安全区域。如果接口不加入安全区域，会导致业务不通。

```
[Clean] firewall zone trust
[Clean-zone-trust] add interface GigabitEthernet 1/0/1
[Clean-zone-trust] add interface GigabitEthernet 1/0/2
[Clean-zone-trust] add interface GigabitEthernet 2/0/1
[Clean-zone-trust] add interface GigabitEthernet 2/0/2
[Clean-zone-trust] add interface GigabitEthernet 3/0/0
[Clean-zone-trust] quit
```

步骤 5　打开域间缺省包过滤。

在缺省情况下，禁止通过清洗设备的各域间安全策略，需要配置域间包过滤为允许，报文才能正常通过清洗设备。在清洗设备上，可以不配置严格安全策略，把所有安全策略打开即可。

```
[Clean] security-policy
[Clean-policy-security] default action permit
[Clean-policy-security] quit
```

步骤 6　配置 SNMP V3 功能。

我们要同时在清洗设备和 ATIC 上配置 SNMP 功能，并保证配置参数一致，这样 ATIC 才可以获取清洗设备的状态信息。

```
[Clean] acl 2998
[Clean-acl-basic-2998] rule permit source 10.1.6.2 0 description for snmp access
[Clean-acl-basic-2998] quit
[Clean] snmp-agent acl 2998
[Clean] snmp-agent sys-info version v3
[Clean] snmp-agent group v3 atic privacy acl 2998
[Clean] snmp-agent usm-user v3 atic
[Clean] snmp-agent usm-user v3 atic group atic
[Clean] snmp-agent usm-user v3 atic authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[Clean] snmp-agent usm-user v3 atic privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
```

步骤 7　配置清洗口。

清洗口一般指的是待清洗流量进入清洗设备的接口。在旁路部署的场景中，清洗口是引流流量的入口。从这个接口进入清洗设备的流量，都要经过清洗模块，所以需要在接口上指定接口类型并配置流量统计功能。

流量统计功能是清洗设备对流量进行清洗的前提条件，在清洗口务必开启流量统计功能，否则清洗功能不生效。在缺省情况下，接口流量统计功能为关闭状态。

```
[Clean] interface GigabitEthernet 1/0/1
[Clean-GigabitEthernet1/0/1] anti-ddos clean enable
[Clean-GigabitEthernet1/0/1] anti-ddos flow-statistic enable
[Clean-GigabitEthernet1/0/1] quit
[Clean] interface GigabitEthernet 2/0/1
[Clean-GigabitEthernet2/0/1] anti-ddos clean enable
```

```
[Clean-GigabitEthernet2/0/1] anti-ddos flow-statistic enable
[Clean-GigabitEthernet2/0/1] quit
```

步骤 8　在清洗设备上，配置生成 UNR 时使用的下一跳地址建议配置为虚地址（10.10.10.10）。

在双链路场景中，生成 UNR 使用的下一跳地址建议配置为虚地址。如果配置为回注口直连的路由器接口 IP 地址之一，比如本例中的 10.1.3.1 或者 10.1.1.1（firewall ddos bgp-next-hop10.1.3.1），则可能会有链路可靠性风险，比如在回注口 Down 后，会导致两条链路的 BGP 引流同时失败。

```
<Clean> system-view
[Clean] firewall ddos bgp-next-hop 10.10.10.10
[Clean] ip route-static 10.10.10.10 32 10.1.3.1
[Clean] ip route-static 10.10.10.10 32 10.1.1.1
```

步骤 9　在清洗设备上配置 BGP 功能及团体属性。

```
[Clean] route-policy 1 permit node 1
[Clean-route-policy] apply community no-advertise
[Clean-route-policy] quit
[Clean] bgp 100
[Clean-bgp] peer 10.1.0.1 as-number 100
[Clean-bgp] peer 10.1.2.1 as-number 100
[Clean-bgp] import-route unr
[Clean-bgp] ipv4-family unicast
[Clean-bgp-af-ipv4] peer 10.1.0.1 route-policy 1 export
[Clean-bgp-af-ipv4] peer 10.1.0.1 advertise-community
[Clean-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export
[Clean-bgp-af-ipv4] peer 10.1.2.1 advertise-community
[Clean-bgp-af-ipv4] quit
[Clean-bgp] quit
```

完成上述配置后，清洗设备上生成的 UNR 会被引入到 BGP 中，并通过 BGP 发布到 Router 上。这时，当 Router 收到目的地址为 1.1.1.1/32 的流量时，通过查找路由表，根据最长掩码匹配原则，优先将流量从接口 GE1/0/1 转发至清洗设备。

步骤 10　在清洗设备接口 GE2/0/1 和 GE1/0/1 配置策略路由，实现回注功能。

```
[Clean] policy-based-route
[Clean-policy-pbr] rule name huizhu1
[Clean-policy-pbr-rule-huizhu1] ingress-interface GigabitEthernet 2/0/1
[Clean-policy-pbr-rule-huizhu1] action pbr egress-interface GigabitEthernet 2/0/2 next-hop 10.1.3.1
[Clean-policy-pbr-rule-huizhu1] quit
[Clean-policy-pbr] rule name huizhu2
[Clean-policy-pbr-rule-huizhu2] ingress-interface GigabitEthernet 1/0/1
[Clean-policy-pbr-rule-huizhu2] action pbr egress-interface GigabitEthernet 1/0/2 next-hop 10.1.1.1
[Clean-policy-pbr-rule-huizhu2] quit
[Clean-policy-pbr] quit
```

步骤 11　保存配置，配置时要随时保存，以免丢失。

```
<Clean> save
```

3. 配置 ATIC

步骤 1　登录 ATIC。

① 在浏览器中输入管理中心 IP 地址“https://10.1.6.2”，按“Enter”。

② 在登录界面，输入用户名、密码和验证码。用户名为 admin，密码为 Admin@123，

单击“登录”。

③ 第一次登录，修改初始密码。

步骤 2　创建 Anti-DDoS 设备，将检测设备和清洗设备添加至 ATIC，如图 7-39 和图 7-40 所示。

① 选择“防御 > 网络配置 > 设备”。

② 单击 创建 。

- IP 地址是指 AntiDDoS8000 管理口 IP 地址。
- 日志源 IP 是指 AntiDDoS8000 的日志口 IP 地址。
- 日志密码是指上报日志的加密密钥。当设备创建成功后，ATIC 将密钥下发到 Anti-DDoS 设备上。
- STelnet 的参数和 SNMP 的参数配置要和 AntiDDoS8000 设备的配置必须保持一致，系统会对其进行校验。

③ 单击“确定”。检测设备和清洗设备被成功添加至 ATIC。

创建设备

设备信息

基本信息

设备名称: clean　IP地址: 10.1.6.1

类型: AntiDDoS　日志源IP: 10.1.6.1

日志密码: ●●●●●●●●●●

Telnet参数

类型: STELNET

用户名: atic　密码: ●●●●●●●●●●

公钥:

提示：
1.如果填写了公钥，使用STELNET、SFTP协议访问设备时对设备进行公钥认证。
2.为了保证数据传输的安全性，建议填写公钥。

SNMP参数

类型: SNMPv3　用户名: atic

环境名称:　环境引擎ID:

授权认证协议: HMACSHA　授权认证密码: ●●●●●●●●●●

数据加密协议: AES128　数据加密密码: ●●●●●●●●●●

确定　取消

图 7-39　创建清洗

图 7-40 创建检测设备

步骤 3 选择"防御 > 策略配置 > 防护对象"，创建自定义防护对象，并配置防护对象基本信息。

添加设备时，请同时选中检测设备和清洗设备。

防护对象的 IP 地址为需要保护的服务器 IP 地址，不同业务类型的服务器，创建不同的防护对象。例如，针对 DNS 服务器，创建防护对象 dnsZone。

步骤 4 配置 DNS 服务器的防御策略。

DNS 服务器主要承载 DNS 业务，DNS 业务主要以端口号为 53 和 5060 的 UDP 报文为主，其他端口的 UDP 业务和 TCP 业务报文较少，其他类型的报文也很少，所以精细化防御以 DNS 防御策略为主。

① 选择"防御 > 策略配置 > 防护对象"，单击防护对象 dnsZone 对应的 。

② 在"防御策略"页签中，单击以 basic 开头的默认防御策略对应的"操作"列的 。

③ TCP 防御：TCP 业务较少，配置以限速为主，如图 7-41 所示。

④ UDP 防御：通常，DNS 服务器上除了 53 和 5060 以外的其他端口 UDP 业务比较少，UDP 限速正是针对除 53 和 5060 以外的其他端口 UDP 进行的，所以可开启限速

功能，如图 7-42 所示。



图 7-41　TCP 防御策略的配置

配置防御策略
TCP　UDP　ICMP　Other　DNS　SIP　HTTP　HTTPS　Top N学习　首包检查
阻断
限流
UDP限流
带宽阈值 (Mbps): 10 * (1-2000000)
UDP分片限流
带宽阈值 (Mbps): 60 * (1-2000000)
UDP新建会话限速
限速阈值 (连接数/秒): 10000 (1-400000)
防御
导入策略模板　导出策略模板　确定　取消

图 7-42　UDP 防御策略的配置

⑤ ICMP 防御：在现网中，正常情况下只有少量的 Ping 报文，所以 ICMP 的限速阈值可以配置小一点，如图 7-43 所示。

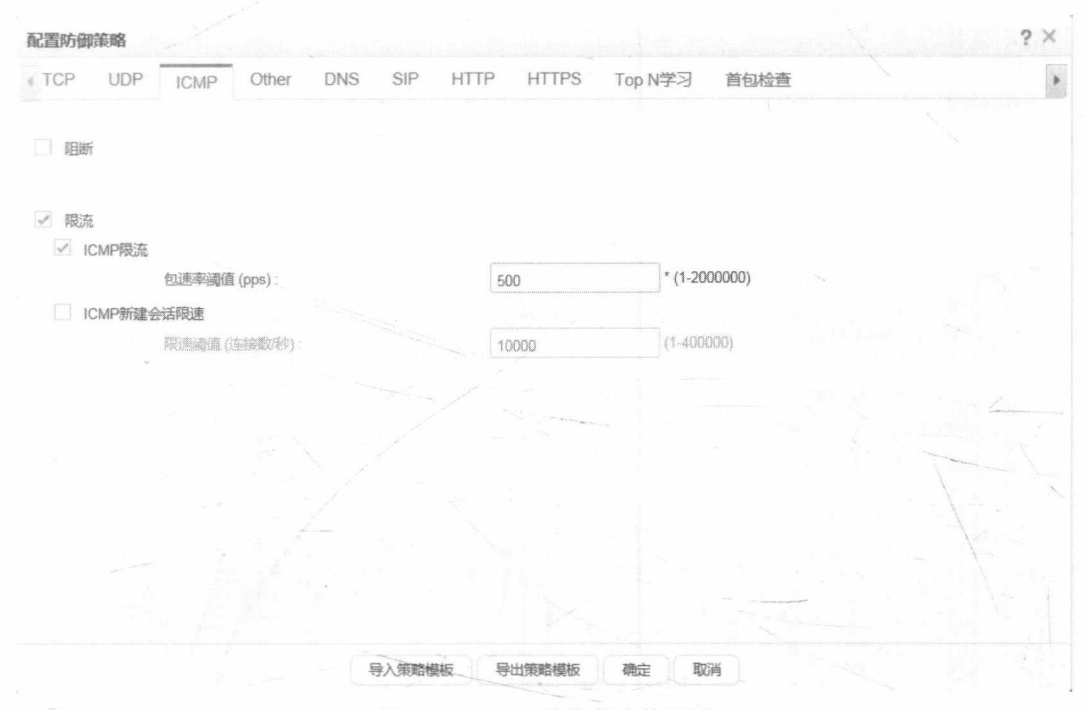


图 7-43 ICMP 防御策略的配置

⑥ Other 报文的防御以限流为主，如图 7-44 所示。

配置防御策略

TCP UDP ICMP Other DNS SIP HTTP HTTPS Top N学习 首包检查

阻断

限流

Other限流

带宽阈值 (Mbps) : 5 * (1-2000000)

Other新建会话限速

限速阈值 (连接数/秒) : 10000 (1-400000)

防御

导入策略模板 导出策略模板 确定 取消

图 7-44 Other 防御策略的配置

⑦ DNS 防御：针对 DNS 服务器的类型配置精细化防御策略，如图 7-45 所示。



图 7-45　DNS 防御策略的配置

⑧ HTTP 源认证防御，如图 7-46 所示。

配置防御策略

TCP　UDP　ICMP　Other　DNS　SIP　HTTP　HTTPS　Top N学习　首包检查

防御

HTTP防御
基于目的IP统计
包速率阈值 (pps)　8000　* (1-80000000)
请求速率阈值 (qps)　4000　* (1-80000000)
基于源IP统计
包速率阈值 (pps)：　0　* (0-80000000)
请求速率阈值 (qps)：　0　* (0-80000000)
HTTP源认证防御
防御模式：　302重定向　验证码　cookie源认证　JavaScript重定向
验证码输入框标题设置　*
代理检测
源认证终止条件
最大尝试次数 (次)：　100　* (3-1000)
尝试时间 (秒)：　30　* (1-300)
syn报文限速　100　* (1-80000000)

导入策略模板　导出策略模板　确定　取消

图 7-46　HTTP 防御策略的配置

⑨ HTTPS 源认证防御，如图 7-47 所示。

图 7-47　HTTPS 防御策略的配置

⑩ 过滤器配置：除上述防御策略以外，对于不提供服务的端口，可以通过配置过滤器进行阻断。

单击“过滤器”页签，单击 关联过滤器 。选中 ATIC 缺省提供的除“DNS_Amplification”之外的所有过滤器模板，单击“确定”。

步骤 5　部署防御策略。

① 选择“防御 > 策略配置 > 防护对象”，选中防护对象前的复选框，单击 部署。

② 单击“确定”，显示部署的进度提示，完成部署后进度提示自动关闭。

步骤 6　基线学习。

选择“防御 > 策略配置 > 防护对象”，单击“基线学习状态”列的具体状态，开启基线学习功能，如图 7-48 所示。

基线学习不需要配置策略，只要有流量经过设备即可。

步骤 7　调整阈值。

一般情况下，如果应用基线学习的数据后，出现的告警比较多，则需要对阈值或者其他参数进行适当调整。

① 将抽样比调整为 0，即统计每个报文。如果抽样比配置过大，当流量比较小的时候，统计出来的值容易失真和跳变。一般情况下，如果总流量小于 1GB，都可以将抽样比配置为 0。

② 查看该防护对象的流量 TopN（无攻击的情况下），选取流量最大的 IP，并以此 IP 查看各种协议的流量对比（统计方式选择峰值），时间跨度选择一周即可。然后使用每种流量峰值的 2 倍数值作为相应防范的阈值。如果流量峰值比较小，比如只有几十 pps，

建议直接使用默认值作为阈值。

图 7-48　基线学习

步骤 8　保存配置。

① 选择“防御 > 策略配置 > 设备全局配置”，选中 Anti-DDoS 设备前的复选框，单击 保存设备配置 。

② 单击“确定”，显示保存的进度，完成保存后，进度提示自动关闭。

4. Router1 的配置过程

下面以华为路由器 NE80E 为例，介绍 Router1 的 BGP 和策略路由的配置过程。不同版本的路由器配置不同，请根据实际路由器版本进行配置，以下配置仅供参考。

步骤 1　配置 Router1 接口的 IP 地址。

步骤 2　配置 Router1 的 BGP 功能。

```
[Router1] bgp 100
[Router1-bgp] peer 10.1.0.2 as-number 100
[Router1-bgp] quit
```

步骤 3　在 Router1 接口 GE1/0/2 配置策略路由。

定义流分类。

```
[Router1] acl 3001
[Router1-acl-adv-3001] rule permit ip
[Router1-acl-adv-3001] quit
[Router1] traffic classifier class1
[Router1-classifier-class1] if-match acl 3001
[Router1-classifier-class1] quit
```

配置流行为并配置报文转发动作。

```
[Router1] traffic behavior behavior1
[Router1-behavior-behavior1] redirect ip-nexthop 10.1.4.2 interface GigabitEthernet 1/0/3
[Router1-behavior-behavior1] quit
```

定义流量策略并在策略中为类指定行为。

```
[Router1] traffic policy policy1
[Router1-trafficpolicy-policy1] classifier class1 behavior behavior1
[Router1-trafficpolicy-policy1] quit
```

在接口上应用策略路由。

```
[Router1] interface GigabitEthernet 1/0/2
[Router1-GigabitEthernet1/0/2] traffic-policy policy1 inbound
[Router1-GigabitEthernet1/0/2] quit
```

5. Router2 的配置过程

下面以华为路由器 NE80E 为例，介绍 Router2 的 BGP 和策略路由的配置过程。不同版本的路由器配置不同，请根据实际路由器版本进行配置，以下配置仅供参考。

步骤 1 配置 Router2 接口的 IP 地址。

步骤 2 配置 Router2 的 BGP 功能。

```
[Router1] bgp 100
[Router1-bgp] peer 10.1.2.2 as-number 100
[Router1-bgp] quit
```

步骤 3 在 Router2 接口 GE1/0/2 配置策略路由。

定义流分类。

```
[Router1] acl 3001
[Router1-acl-adv-3001] rule permit ip
[Router1-acl-adv-3001] quit
[Router1] traffic classifier class1
[Router1-classifier-class1] if-match acl 3001
[Router1-classifier-class1] quit
```

配置流行为并配置报文转发动作。

```
[Router1] traffic behavior behavior1
[Router1-behavior-behavior1] redirect ip-nexthop 10.1.5.2 interface GigabitEthernet 1/0/3
[Router1-behavior-behavior1] quit
```

定义流量策略并在策略中为类指定行为。

```
[Router1] traffic policy policy1
[Router1-trafficpolicy-policy1] classifier class1 behavior behavior1
[Router1-trafficpolicy-policy1] quit
```

在接口上应用策略路由。

```
[Router1] interface GigabitEthernet 1/0/2
[Router1-GigabitEthernet1/0/2] traffic-policy policy1 inbound
[Router1-GigabitEthernet1/0/2] quit
```

7.4　企业园区防护

随着网络技术的不断发展以及网络的广泛应用，企业园区作为最广泛的应用网络，面临着越来越多的攻击。企业园区既要抵御来自外网的黑客攻击、病毒攻击、DDoS 攻击、木马攻击、恶意程序攻击，还要确保业务应用畅通，如图 7-49 所示。

针对企业园区流量特点，在规划时从以下几个方面考虑。

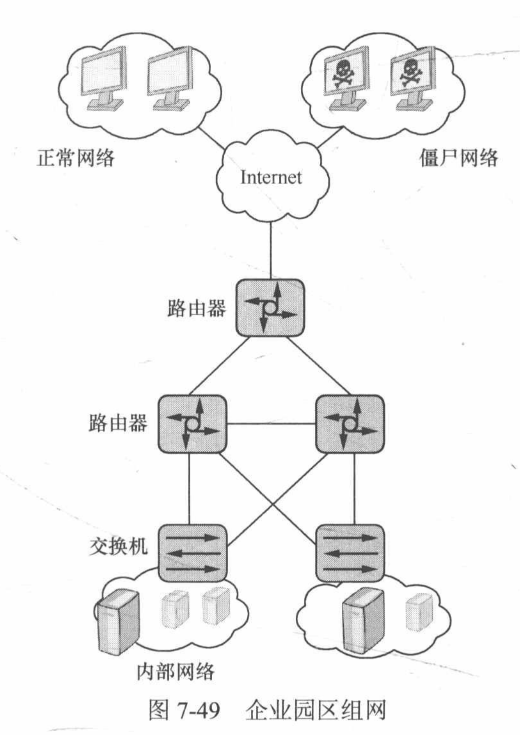


图 7-49　企业园区组网

7.4.1　规划思路

（1）设备选择

从检测技术方面考虑，在通常情况下，企业园区的网络规模比较小，带宽不大（小于 5Gbit/s），如果采用逐流检测，在流量比较小的情况下，统计结果容易失真。所以为了保证检测的精准度，并结合网络带宽情况，推荐使用可以逐包检测的华为 AntiDDoS1600 设备。

AntiDDoS1600 系列设备包含两个型号的产品：AntiDDoS1650 和 AntiDDoS1680。两个产品均为集中式设备形态，但一个是 1U 设备，一个是 3U 设备，两者性能不同。

从商务方面考虑，AntiDDoS1600 是华为的中低端 AntiDDoS 产品，成本低，功能全，适合小型企业园区采购。

（2）部署方式

AntiDDoS1600 支持内置 Bypass 卡，直路部署方式可以满足基本的网络需求。AntiDDoS1600 作为清洗设备以透明模式直路接入，不影响网络拓扑；同时内置 Bypass

卡，提供两条 Bypass 链路。

当 AntiDDoS1600 正常工作时，一对 Bypass 接口不直接连通，流量经过 AntiDDoS1600 设备处理；当 AntiDDoS1600 下电或者出现故障时，上、下游设备通过一对 Bypass 接口直连，流量不经过 AntiDDoS1600 设备处理。这样确保了业务不会被中断，可靠性增强，避免出现单点故障。

在直路部署方式中，所有报文实时经过 AntiDDoS1600，AntiDDoS1600 可对报文进行实时统计和检测，一旦发生攻击，立即启动防御，没有延时。直路部署无需部署检测设备。

（3）流量引导方式

直路部署流量，不涉及引流回注。

（4）License 控制

AntiDDoS1600 不支持 License 控制。

AntiDDoS1600 有两种设备形态：检测设备和清洗设备。设备出厂时，缺省是清洗设备，可以通过命令行配置，由清洗设备切换为检测设备。

（5）接口规划

由于是直路部署，因此 AntiDDoS1600 设备 Bypass 卡上的接口与上下行设备相连。除此之外，AntiDDoS1600 还要规划一个管理口和一个日志口，与 ATIC 互通。

作为清洗设备，AntiDDoS1600 与 ATIC 通信的管理接口和日志接口，可以是同一接口，也可以是不同接口。任何接口均可作为与 ATIC 通信的管理接口及发送日志的接口。为了避免发生攻击时 CPU 使用率过高，设备托管，建议管理口用 GigabitEthernet0/0/0，日志口用另外一个单独的接口。

如果 AntiDDoS1600 作为检测设备，只能用 GigabitEthernet0/0/0 作为与 ATIC 通信的管理接口和发送日志的接口。本案例中 AntiDDoS1600 不作为检测设备。

（6）防御策略

首先明确设备要防护的目标 IP，针对目标建立防护对象，然后配置相应的防护策略。对于其他不明确的目标，配置默认防护对象的防御策略来防御。

例如，网络中有 3 台 Web 服务器、2 台 DNS 服务器以及 5 台游戏服务器。不同的服务器配置不同的防御策略，像 Web 服务器重点配置 HTTP 类的防御策略，DNS 服务器则重点配置 DNS 类的防御策略，游戏服务器则重点配置 UDP/TCP 类的防御策略。

如果我们为每一个服务器建立一个防护对象，则需要建立 10 个防护对象，配置起来比较麻烦。如果同一类型的服务器业务基本相同，则可以只配置 3 个防护对象，即针对 Web 服务器、DNS 服务器和游戏服务器的 3 个防护对象；然后，在每一个防护对象中将多个服务器的 IP 地址添加进来（每个防护对象可以配置多个 IP 或者网段）；最后，再配置相应的防御策略，这样每一类服务器只需要配置一次策略。

配置完成后，就完成了对重点目标的防护，我们也可以对企业园区中其他的网络资源使用默认防护对象的防御策略进行防御。

（7）安全策略规划

在缺省情况下，AntiDDoS1600 设备上的安全策略是关闭的，但可以打开缺省包过滤。

（8）ATIC

ATIC 由管理中心服务器和采集器两部分组成，并有两种部署方式。

① 集中式部署：ATIC 服务器和采集器同时安装在同一台物理服务器上。

② 分布式部署：ATIC 服务器和采集器分别安装在不同的物理服务器上，多台采集器可以共用一台 ATIC 服务器，一台 ATIC 服务器最多可管理 20 台采集器。

一台采集器可以处理大约 30 万个 IP 地址的 Anti-DDoS 业务日志，可以根据防护对象的 IP 地址个数来选择 ATIC 部署方式。设备旁路部署时，如果多台设备部署地比较分散，建议配置多台采集器。

在本例中，采用 ATIC 集中式部署即可满足组网需求。

（9）路由规划

清洗设备和 ATIC 之间要路由可达。

7.4.2 典型组网

如图 7-50、图 7-51 所示，AntiDDoS1600 设备（清洗设备）直路部署在企业入口处，对进入企业园区的流量进行实时检测。一旦出现攻击，AntiDDoS1600 设备立即启动防御措施，对流量进行清洗，阻断攻击流量，转发正常流量。



当清洗设备正常工作时，清洗设备先处理所有流量，再转发

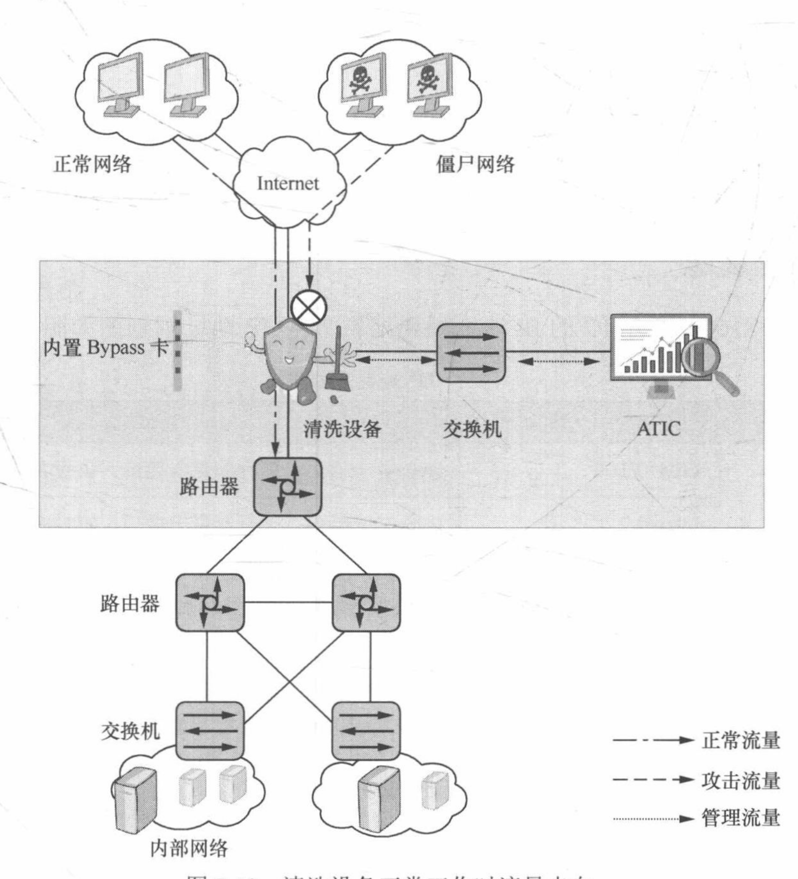


图 7-50　清洗设备正常工作时流量走向



当清洗设备故障或下电时，所有流量直接由 Bypass 卡转发，清洗设备不再处理

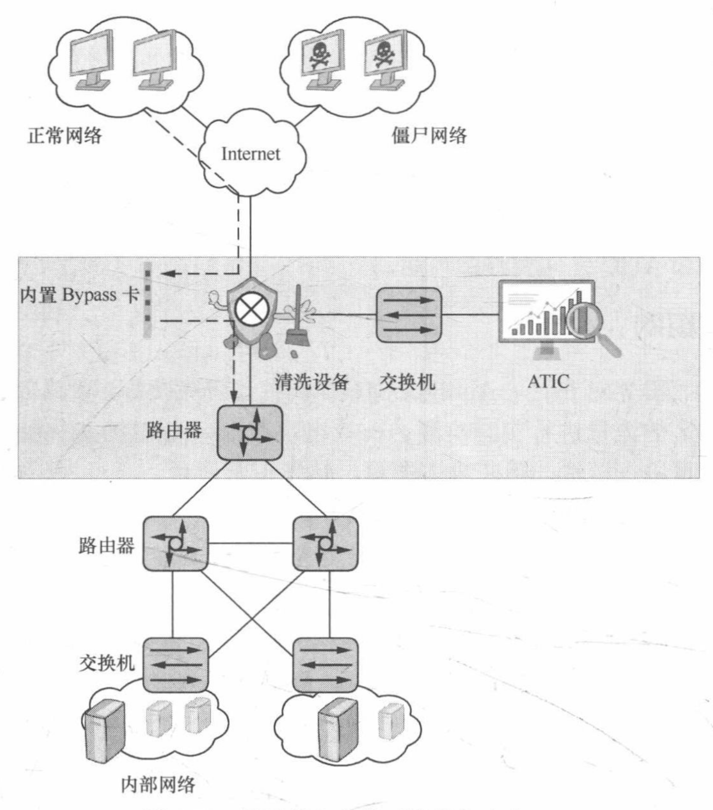


图 7-51 清洗设备故障时流量的走向

7.4.3 数据规划

AntiDDoS1600 和 ATIC 的 IP 地址规划见表 7-7。IP 地址规划图如图 7-52 所示。

表 7-7 IP 地址规划表

设备名称	接口	IP 地址	说明
AntiDDoS1600 设备	GE1/0/1	-	Bypass 卡接口，下行流量入接口，该设备与上游设备直连
	GE1/0/2	-	Bypass 卡接口，下行流量出接口，该设备与下游设备直连
	GE0/0/0	10.1.6.1/24	管理口。用于 ATIC 管理 AntiDDoS1600 设备。此接口 IP 地址与管理中心 IP 地址必须路由可达，本案例中，此接口 IP 地址与管理中心在同一网段
	GE2/0/0	10.1.7.1/24	日志口。用于 AntiDDoS1600 设备向 ATIC 发送日志。AntiDDoS1600 设备将日志报文/抓包报文发送至管理中心的 Anti-DDoS 采集器，供 Anti-DDoS 采集器分析以及进行后续处理。 此接口 IP 地址与管理中心 IP 地址必须路由可达
ATIC	–	10.1.6.2/24	管理中心与 AntiDDoS1600 设备路由可达

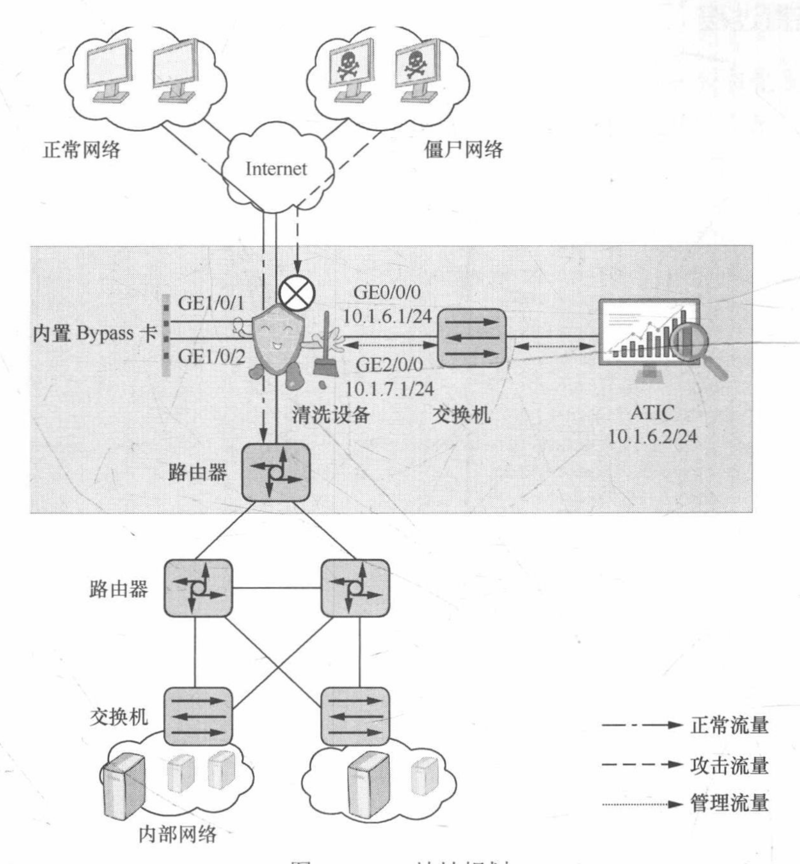


图 7-52　IP 地址规划

7.4.4　配置思路

1. 在 AntiDDoS1600 设备上需要完成以下主要功能的配置

① 在二层配置上、下行接口。

② 接口加入安全区域，并打开域间缺省包过滤。

③ 配置与 ATIC 通信的管理口 IP 地址和日志口 IP 地址。

④ 配置 STelnet 功能。

⑤ 配置 SNMP 功能，使管理中心可以获取 AntiDDoS1600 设备的状态。

⑥ 在 AntiDDoS1600 设备的流量入接口开启流量统计功能。

⑦ 保存配置。

2. ATIC 需要完成以下主要功能的配置

① 登录 ATIC。

② 创建 Anti-DDoS。

③ 配置相应的防御策略。

④ 配置基线学习功能，并对防御阈值进行调整。

⑤ 保存配置。

7.4.5 配置过程

1. 配置清洗设备

步骤 1 在二层配置上、下行接口，并将各接口加入相应的安全区域。

在直路部署 Bypass 的场景中，与上、下行设备直连的接口使用 Bypass 卡上的接口。上、下行接口工作在二层，无须配置 IP 地址。

```
[AntiDDoS] interface GigabitEthernet 1/0/1
[AntiDDoS-GigabitEthernet1/0/1] undo service-manage enable
[AntiDDoS-GigabitEthernet1/0/1] portswitch
[AntiDDoS-GigabitEthernet1/0/1] port link-type access
[AntiDDoS-GigabitEthernet1/0/1] port default vlan 1000
[AntiDDoS-GigabitEthernet1/0/1] quit
[AntiDDoS] interface GigabitEthernet 1/0/2
[AntiDDoS-GigabitEthernet1/0/2] undo service-manage enable
[AntiDDoS-GigabitEthernet1/0/2] portswitch
[AntiDDoS-GigabitEthernet1/0/2] port link-type access
[AntiDDoS-GigabitEthernet1/0/2] port default vlan 1000
[AntiDDoS-GigabitEthernet1/0/2] quit
```

步骤 2 配置日志口和管理口 IP 地址。

在本案例中，AntiDDoS1600 的日志口和管理口分离，并分别设置为不同的接口。后续在 ATIC 创建设备时，会具体指定哪个接口是管理口，哪个接口是日志口。

```
[AntiDDoS] interface GigabitEthernet 2/0/0
[AntiDDoS-GigabitEthernet2/0/0] undo service-manage enable
[AntiDDoS-GigabitEthernet2/0/0] ip address 10.1.7.1 24
[AntiDDoS-GigabitEthernet2/0/0] quit
[AntiDDoS] interface GigabitEthernet 0/0/0
[AntiDDoS-GigabitEthernet0/0/0] undo service-manage enable
[AntiDDoS-GigabitEthernet0/0/0] ip address 10.1.6.1 24
[AntiDDoS-GigabitEthernet0/0/0] quit
```

步骤 3 接口加入安全区域。如果接口不加入安全区域，则会导致业务不通。

```
[AntiDDoS] firewall zone trust
[AntiDDoS-zone-trust] add interface GigabitEthernet 1/0/1
[AntiDDoS-zone-trust] add interface GigabitEthernet 1/0/2
[AntiDDoS-zone-trust] add interface GigabitEthernet 2/0/0
[AntiDDoS-zone-trust] add interface GigabitEthernet 0/0/0
[AntiDDoS-zone-trust] quit
```

步骤 4 打开域间缺省安全策略。

在缺省情况下，AntiDDoS1600 的各域间安全策略是禁止通过的，需要配置域间包过滤为允许，报文才能正常通过 AntiDDoS1600 设备。在 AntiDDoS1600 上，可以不配置严格安全策略，把所有安全策略打开即可。

```
[AntiDDoS] security-policy
[AntiDDoS-policy-security] default action permit
[AntiDDoS-policy-security] quit
```

步骤 5 配置 STelnet 功能。

配置 STelnet 功能是为了实现 ATIC 对 AntiDDoS1600 设备的管理，比如防御策略的下发、引流策略的下发等。ATIC 和 AntiDDoS1600 设备中 STelnet 参数的配置要保持完全一致。

```
[AntiDDoS] user-interface vty 0 4
[AntiDDoS-ui-vty0-4] authentication-mode aaa
```

```
[AntiDDoS-ui-vty0-4] user privilege level 3
[AntiDDoS-ui-vty0-4] protocol inbound ssh
[AntiDDoS-ui-vty0-4] quit
[AntiDDoS] aaa
[AntiDDoS-aaa] manager-user atic
[AntiDDoS-aaa-manager-user-atic] password
Enter Password:
Confirm Password:
[AntiDDoS-aaa-manager-user-atic] service-type ssh
[AntiDDoS-aaa-manager-user-atic] level 15
[AntiDDoS-aaa-manager-user-atic] quit
[AntiDDoS-aaa] quit
[AntiDDoS] rsa local-key-pair create
The key name will be: AntiDDoS_Host
The range of public key size is (512 ~ 2048).
NOTES: A key shorter than 1024 bits may cause security risks.
        The generation of a key longer than 512 bits may take several minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
...++++++++
..++++++++
.................................+++++++++
...........+++++++++
[AntiDDoS] stelnet server enable
[AntiDDoS] ssh user admin
[AntiDDoS] ssh user atic authentication-type password
[AntiDDoS] ssh user atic service-type stelnet
```

步骤 6　配置 SNMP V3 功能。

要同时在 AntiDDoS1600 设备和 ATIC 配置 SNMP 功能，并确保配置参数一致，这样 ATIC 才可以获取 AntiDDoS1600 设备的状态信息。

```
[AntiDDoS] acl 2998
[AntiDDoS-acl-basic-2998] rule permit source 10.1.6.2 0 description for snmp access
[AntiDDoS-acl-basic-2998] quit
[AntiDDoS] snmp-agent acl 2998
[AntiDDoS] snmp-agent sys-info version v3
[AntiDDoS] snmp-agent group v3 atic privacy acl 2998
[AntiDDoS] snmp-agent usm-user v3 atic
[AntiDDoS] snmp-agent usm-user v3 atic group atic
[AntiDDoS] snmp-agent usm-user v3 atic authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[AntiDDoS] snmp-agent usm-user v3 atic privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
```

步骤 7　配置流量统计功能。

流量统计功能是清洗设备对流量进行清洗的前提条件，在清洗口务必开启流量统计功能，否则清洗功能不生效。在缺省情况下，接口流量统计功能为关闭状态。

```
[AntiDDoS] interface GigabitEthernet 1/0/1
[AntiDDoS-GigabitEthernet1/0/1] anti-ddos flow-statistic enable
[AntiDDoS-GigabitEthernet1/0/1] quit
```

步骤 8　保存配置。

```
<AntiDDoS> save
```

2. 配置 ATIC

步骤 1 登录 ATIC。

① 在浏览器中输入管理中心 IP 地址，按“Enter”。

在登录界面输入用户名、密码和验证码。初始用户名为 admin，密码为 Admin@123，单击“登录”。在第一次登录后，请修改初始密码。

步骤 2 创建 Anti-DDoS。

① 选择“防御 > 网络配置 > 设备”，如图 7-53 所示。

② 单击 创建 。

- IP 地址是指 AntiDDoS1600 管理口的 IP 地址。
- 日志源 IP 是指 AntiDDoS1600 的日志口 IP 地址。
- 日志密码是指上报日志的加密密钥。当创建设备成功后，ATIC 将密钥下发到 AntiDDoS1600 设备上。
- STelnet 的参数和 SNMP 的参数配置与 AntiDDoS1600 设备的配置必须保持一致，系统会对其进行校验。

③ 单击“确定”。AntiDDoS1600 设备被成功添加到设备列表中。

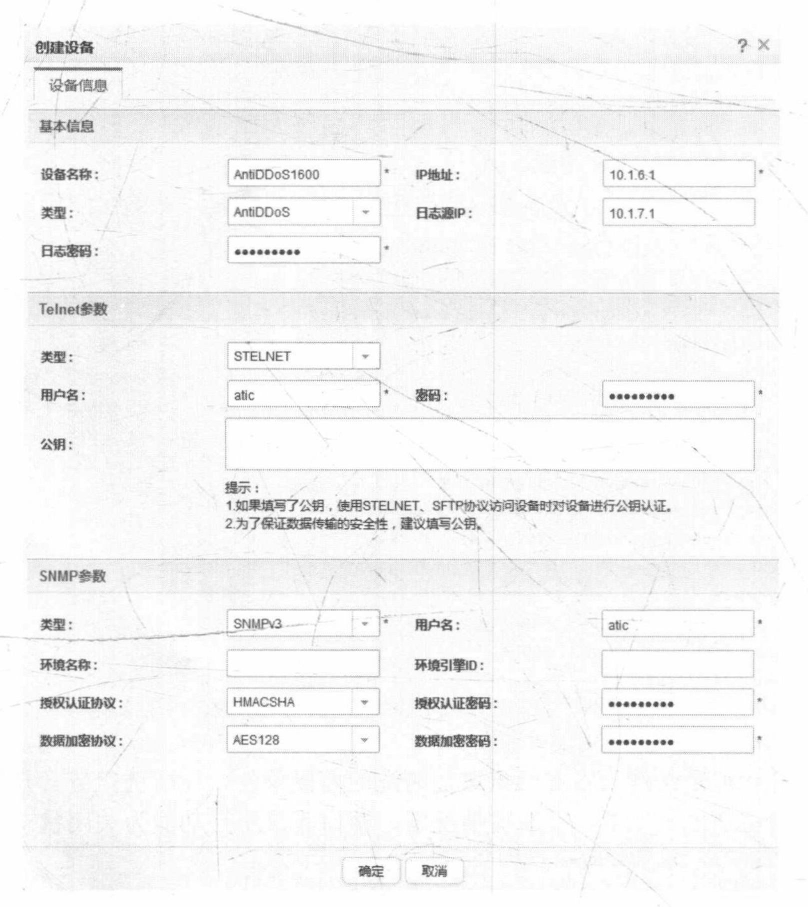


图 7-53 创建 Anti-DDoS

步骤 3 选择“防御 > 策略配置 > 防护对象”，创建自定义防护对象，并配置防护对

象基本信息。

步骤4　配置防御策略。

在配置防御策略时，先甄别出需要重点保护的目的IP地址，加入到自定义防护对象中，并基于自定义防护对象配置相应的防御策略；对于不确定是否要保护的目的IP地址，则用默认防护对象防御策略进行保护。防御策略的配置要结合实际网络业务的特征进行配置，下面以通用防御策略进行介绍，仅作参考。现网配置时，请根据实际情况进行调整。

① 选择"防御 > 策略配置 > 防护对象"，创建并单击默认防护对象对应的，配置防御模式，如图7-54所示。

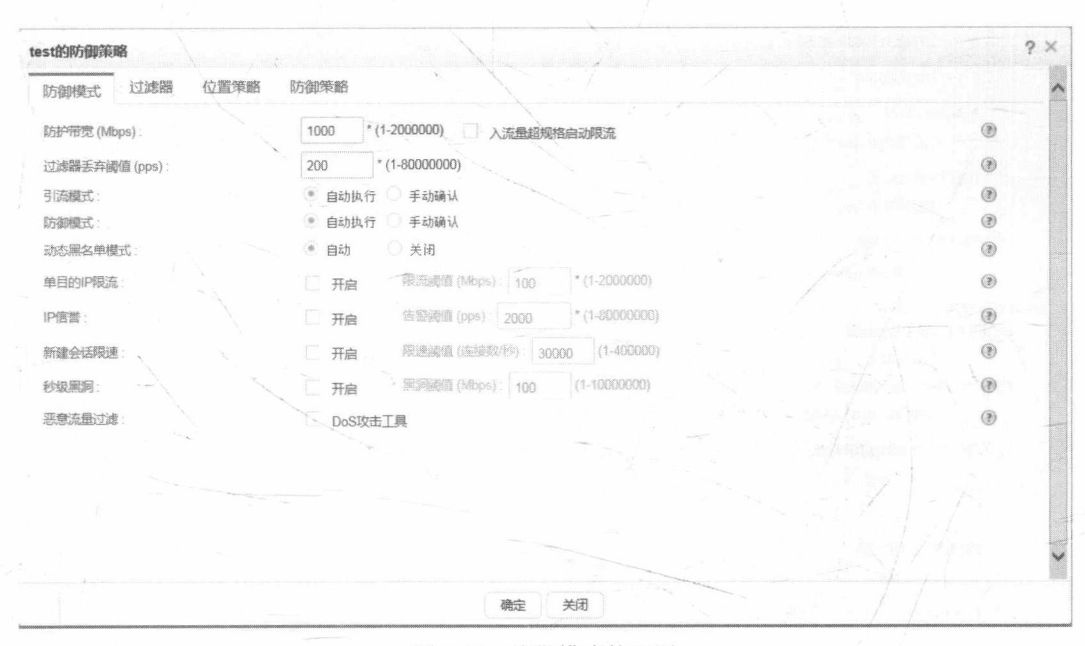


图7-54　防御模式的配置

② 在"防御策略"页签中，单击以basic开头的默认防御策略对应的"操作"列的。

③ 配置TCP通用防御策略。防御阈值可以根据基线学习的结果进行调整，如图7-55所示。

配置ACK Flood防御时，严格模式的防御效果优于宽松模式的防御效果。

• 在直路部署时，推荐使用严格模式。业务不会出现中断，防御效果也要优于宽松模式。

• 在旁路部署时，建议使用宽松模式。如果在旁路部署时使用严格模式，根据严格模式防御原理，业务在引流后，ACK报文命中的会话必须是由SYN或SYN-ACK建立，否则报文会被丢弃，在会话重建后业务才会正常运行。

配置防御策略

TCP UDP ICMP Other DNS SIP HTTP HTTPS Top N学习 首包检查

防御
TCP异常报文防御
包速率阈值 (pps): 1000 * (1-80000000)
TCP基本防御
SYN Flood防御
认证模式: error-seq right-seq
包速率阈值 (pps): 2000 * (1-80000000)
源IP SYN报文比例异常限速
SYN-Ratio比例阈值 (%): 50 * (0-100)
检查周期 (秒): 5 * (1-600)
SYN报文个数限速阈值 (个): 200 * (0-80000000)
限速周期 (秒): 10 * (1-600)
ACK Flood防御
包速率阈值 (pps): 20000 * (1-80000000)
TCP分片攻击防御
包速率阈值 (pps): 2000 * (1-80000000)
FIN/RST Flood防御
包速率阈值 (pps): 500 * (1-80000000)
TCP连接耗尽攻击防御
目的IP地址并发连接数检查
连接数阈值: 5000 * (1-80000000)
目的IP地址新建连接速率检查
连接速率阈值 (连接数/秒): 1000 * (1-10000000)
源IP地址新建连接速率检查
连接数阈值: 200 * (1-80000000)
检查周期 (秒): 5 * (1-60)
源IP地址连接数检查
连接数阈值: 500 * (1-80000000)
异常会话检查
异常连接数阈值: 30 * (1-255)
检查周期 (秒): 15 * (1-240)
空连接检查
每次连接最小报文数: 1 * (1-255)
检查周期 (秒): 30 * (1-240)
重传会话检查
重传报文阈值: 200 * (1-1023)
Sockstress
TCP窗口大小阈值 (字节): 10 * (1-65535)

导入策略模板 导出策略模板 确定 取消

图 7-55 TCP 防御策略的配置

④ 图 7-55 中的配置在攻击时仅能告警，只有配置动态黑名单功能才能进行流量清洗，建议在应急的时候再开启动态黑名单功能。开启方法如图 7-56 所示。

图 7-56　开启动态黑名单

⑤ 配置 UDP 通用防御策略，如图 7-57 所示。

图 7-57　UDP 防御策略的配置

⑥ 配置 ICMP 通用防御策略，如图 7-58 所示。



图 7-58 ICMP 防御策略的配置

⑦ 配置 Other 协议通用防御策略，如图 7-59 所示。

如果可以确认访问被保护的网络流量只有 TCP、UDP、ICMP 业务，不包含 IPSec、GRE、IGMP 等其他协议，建议开启限流，防御效果会更好。

如果存在 IPSec、GRE、IGMP 等其他协议，则不能开启限流，否则会影响正常业务。

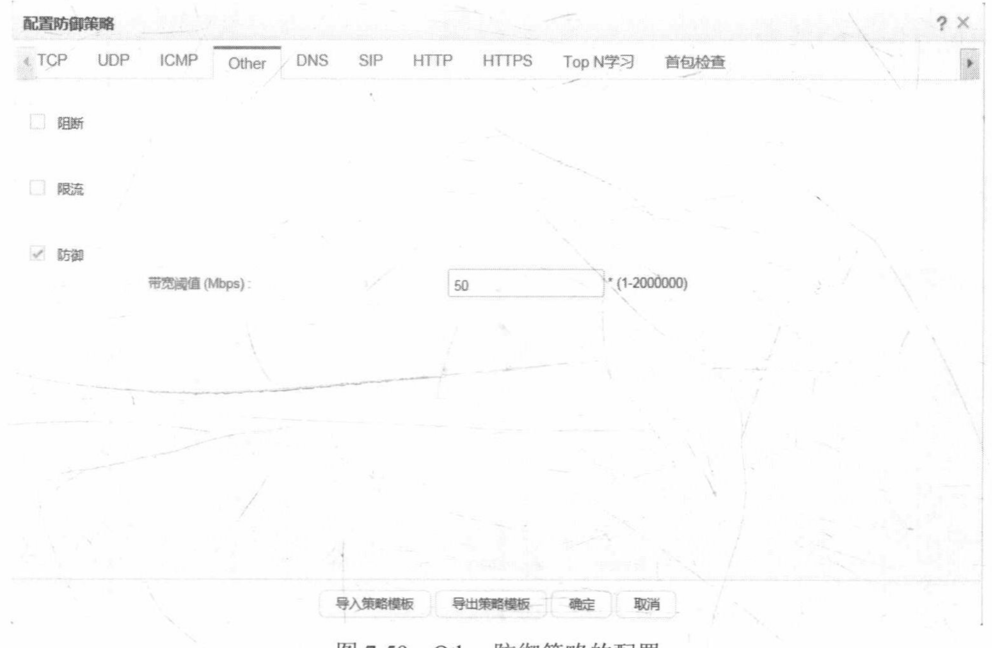


图 7-59 Other 防御策略的配置

⑧ 配置 DNS 协议通用防御策略，如图 7-60 所示。



图 7-60　DNS 防御策略的配置

⑨ 配置 HTTP 协议通用防御策略，如图 7-61 所示。

多数用户的浏览器和 App 都有完整的 HTTP 协议栈，因此可以顺利通过“302 重定向”，当流量超过阈值触发防御后，用户感知不到认证过程，业务访问没有受到任何影响。但少数个别的 App 和程序可能使用不完整的 HTTP 协议栈，无法通过 HTTP“302 重定向”的认证，导致业务受到影响，这时需要关闭 HTTP 源认证防御，避免影响正常业务。

图 7-61　HTTP 防御策略的配置

⑩ 配置 HTTPS 通用防御策略，如图 7-62 所示。

图 7-62 HTTPS 防御策略的配置

⑪ 配置过滤器。对于不提供服务的端口，配置过滤器进行阻断，否则将会影响防御效果。

单击“过滤器”页签，单击 关联过滤器 。选中 ATIC 缺省提供的全部常用过滤器模板，单击“确定”。

步骤 5 部署防御策略。

① 选择“防御 > 策略配置 > 防护对象”，选中防护对象前的复选框，单击部署。

② 单击“确定”，显示部署的进度提示，完成部署后进度提示自动关闭。

步骤 6 基线学习。

选择“防御 > 策略配置 > 防护对象”，单击“基线学习状态”列的具体状态，开启基线学习功能，如图 7-63 所示。

基线学习不需要配置策略，只要有流量经过设备即可。

步骤 7 调整阈值。

在一般情况下，如果应用基线学习的数据后，出现的告警比较多，则需要对阈值或者其他参数进行适当调整。

将抽样比调整为 0，即统计每个报文。如果抽样比配置过大，当流量比较小的时候，统计出来的值容易失真和跳变。在一般情况下，如果总流量小于 1GB，可以将抽样比配置为 0。

查看该防护对象的流量 TopN（无攻击的情况下），选取流量最大的 IP，并以此 IP 查看各种协议的流量对比（统计方式选择峰值），时间跨度选择一周。然后使用每种流量

的峰值的 2 倍作为相应防范的阈值。如果流量峰值比较小，比如只有几十 pps，建议直接使用默认值作为阈值。

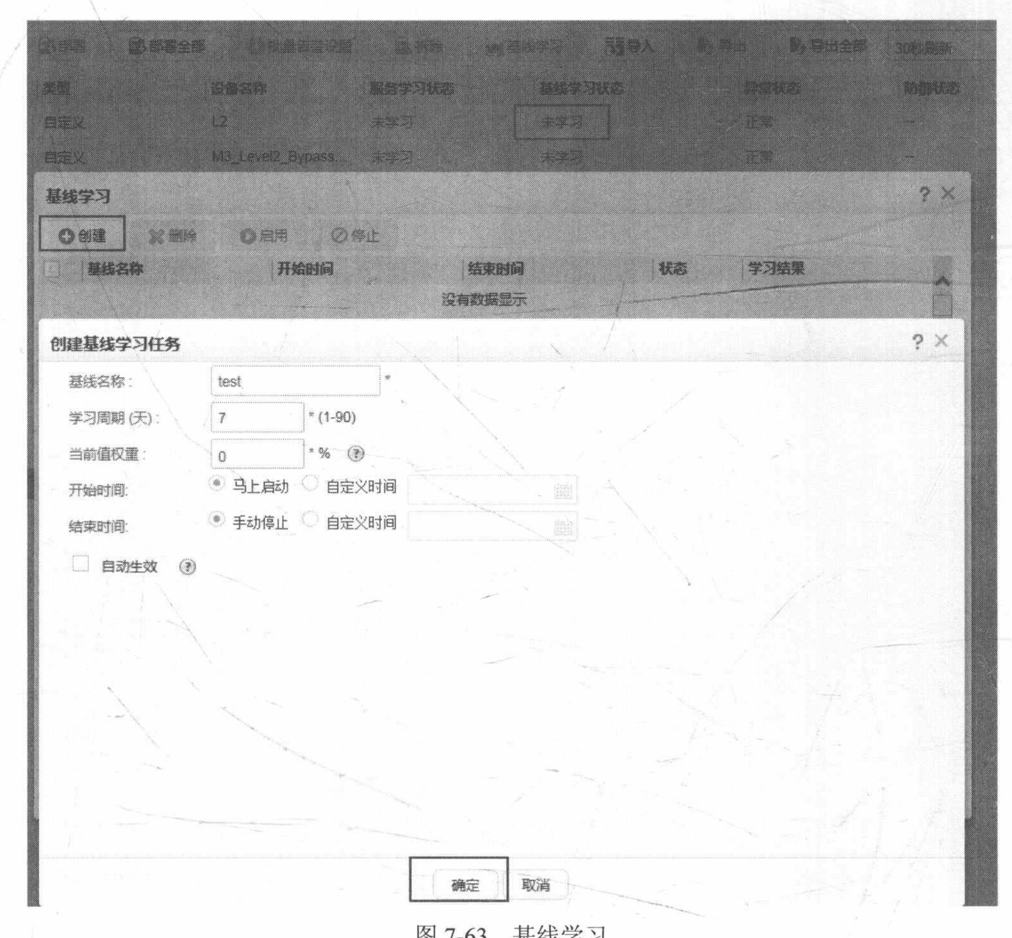


图 7-63　基线学习

步骤 8　保存配置。

① 选择“防御 > 策略配置 > 设备全局配置”，选中 Anti-DDoS 设备前的复选框，单击 保存设备配置 。

② 单击“确定”，显示保存的进度提示，完成保存后进度提示自动关闭。

《华为Anti-DDoS技术漫谈》是由华为技术有限公司组织编写的一本关于华为Anti-DDoS技术的学习工具图书，也是华为ICT认证系列培训教材。本书以华为Anti-DDoS方案为主线，结合近几年的热点攻击事件，全面介绍Anti-DDoS技术的攻击和防御原理，同时结合华为Anti-DDoS技术在解决方案中的应用，系统梳理了各种场景的典型配置案例供读者参考。

本书集系统性、专业性和实用性于一体，既有全面分析现网热点的攻击案例，并结合抓包过程深入介绍各类协议的DDoS攻击和防御原理，又有以Step-by-Step方式的详尽配置，介绍了典型场景的部署和操作过程，层次清晰，由浅入深，通俗易懂，使理论与实践完美结合，学以致用，化繁为简。







ISBN 978-7-115-48754-4

定价：59.00 元

分类建议：计算机安全

人民邮电出版社网址：www.ptpress.com.cn

[General Information]
书名=14474960
SS号=14474960